deftech.scan

October 2023

https://deftech.ch/scans

deftech
defencefuturetechnologies

Dear Reader,

The last edition in that form mentioned a change of format, using single posts – https://deftech.ch/technologies/ - instead of a report format as the present one. If we thought initially that the idea was good, reality showed that the expected interactions were not happening and that the today form had its advantages as well.

However, we have introduced in the back-office a collaborative monitoring platform – https://curebot.fr – that helps us structuring our processes. Therefore, this format might only be temporary while we are learning and progressing in the use of the numerous functionalities.

In the meanwhile, we present you some striking news on the following topics:

We wish you an interesting read.

Foresightly Yours,

Tate Nurkin
OTH Intelligence Group
CEO
tate.nurkin@othintel.com

Dr. Quentin Ladetto
armasuisse S+T
Head of Technology Foresight
quentin.ladetto@armasuisse.ch

1 Applications of AI and data

1.1 German consortium uses "third wave" algorithms to test and improve military systems

The German-Swiss Group has created a "metaverse for the Bundeswehr" known as GhostPlay to support tactical military decision-making at machine speed. (source, source, and source)

Assessment: The GhostPlay consortium is led by German company 21strategies and also includes sensor specialist Hensoldt, Bundeswehr University Hamburg, and Swiss company Borchert Consulting and research. The GhostPlay name combines the two components of the simulation system. "Ghost" is the high-performance simulation environment in which third wave AI algorithms are trained while the "Play" component are the tactics developed and generated through the use of context-aware artificial intelligence. According to Yvonne Hofstetter, CEO of 21strategies, third wave algorithms allow simulated battlefield actors and equipment to develop novel courses of action on their own as opposed to second wave AI, which optimizes human decisions.

The system uses detailed digital twins derived from open-source intelligence, such as geo-intelligence and technical profiles of modern military equipment, to replicate real-world operational environments. Much of the reporting and marketing literature to date is focused on the system's ability to better recognize and respond to complex aerial threats such as drone swarms or in-coming missile. Indeed, *Defense News* reporting from 8 September reports how transferring algorithms tested in the GhostPlay environment could greatly enhance the targeting and sensing capability of Gephard self-propelled anti-air artillery. The Bundeswehr no longer uses the Gephard system but has transferred 46 to Ukraine. Researchers trained the simulated Gephard to engage a range of adversary platforms, including Bayraktar TB2 UAVs, drone swarms and Russian attack helicopters with results that showed the Gephards "learns very fine-granular engagement tactics for different types of threats and even senses when it's important to destroy the target or only disable it."
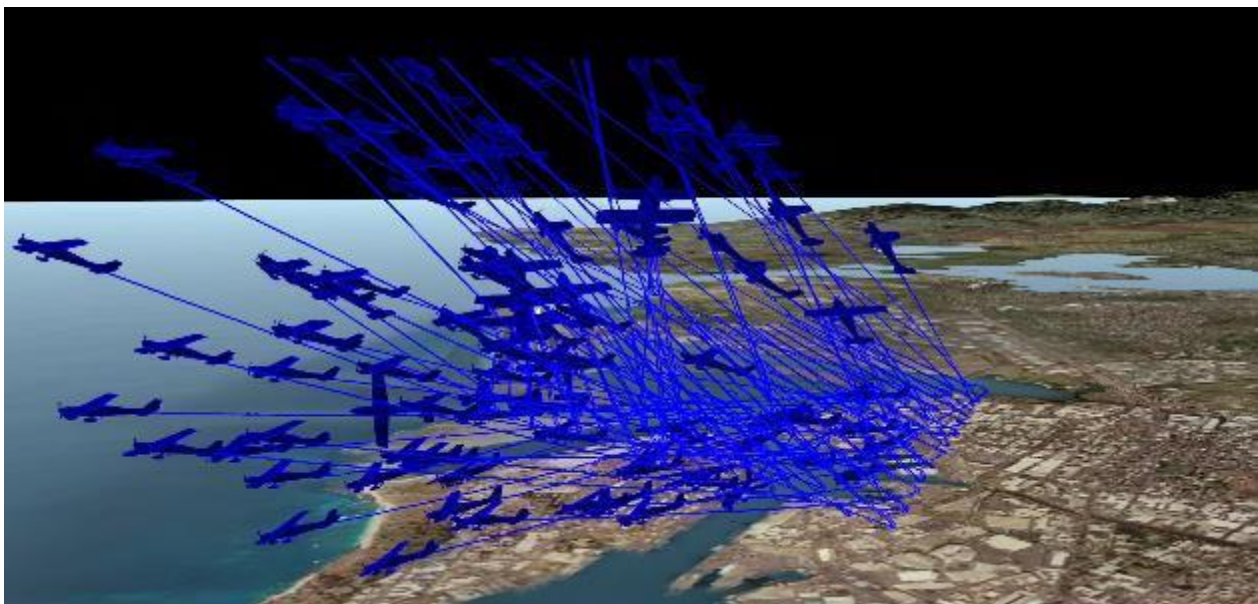

Figure 1: A screen capture from a GhostPlay video (in German) that describes the capability and its value. This screen capture is simulating a drone swarm attack. Source

1.2	**Generative AI and the information / disinformation war**
	Large language models are increasingly featuring in both the crafting of and defence against misinformation and disinformation campaigns over the future of the island of Taiwan ([source](), Meta [report](), and [source]())
	Assessment: While concerns about an armed conflict over Taiwan tend to dominate the discussion of Indo-Pacific security, the People's Republic of China (PRC) is already engaged in a robust effort to shape narratives and opinions on and about the self-governing island as well as other territorial disputes in which the PRC is involved. A Meta [report]() released in August assessed that individuals with known ties to China's law enforcement agencies conducted a massive covert digital influence operation design to discredit the West and parrot PRC talking points about other regional issues and territorial disputes. On Facebook alone, users with ties to the Chinese Communist Party government amassed more than 550,000 followers. Ben Nimo, Meta's Global Threat Intelligence Lead called the campaign "the largest covert influence operation that's currently active in the world today", though the Meta report also indicates that despite its scale the effort has been largely ineffective.
	Taiwan is clearly at the centre of PRC narrative shaping and disinformation campaigns. A recent [RAND Corporation report]() on generative AI and social media manipulation indicates researchers in China are already considering how best to use generative AI tools to amplify the effectiveness and precision of these covert information operations. By convincing a broad segment of the public that more people hold CCP favoured views than actually do, these efforts can synthetically and consequentially influence in debates In addition, generative AI could be used to more rapidly create false news articles and other sources that could create ["a false sense of truth itself."]()
	For its part, Taiwan, is also turning to generative AI to shore up its defences against misinformation and disinformation, especially as the island is preparing for a crucial presidential election in January 2024. Audrey Tang, Taiwan's Minister of Digital Affairs, stated during a September conference in Washington, D.C. that combating disinformation has become a key priority and that a new organization called Cofacts has been established to help in this cause. Users can forward dubious content to Cofacts chatbots. Information is checked by human editors and a verdict is given to the users on the reliability of the content. Generative AI has an important role to play in this counter-disinformation process, especially in helping Taiwan cope with the scale of PRC campaigns. Ms. Tang also noted that ["because gen AI is just so malleable, they just fine-tuned a language model together than can clarify such disinformation . . . adding back a context … So, we're no longer outnumbered."]()

1.3	**US. Department of Defense (DoD) announces intent to start a pilot program to build AI trust**
	The new centre will be called the Center for Calibrated Trust Measurement and Evaluation ([source](#))
	Assessment: The new centre is sponsored by the Office of the Secretary of Defense for Research and Engineering (R&E). Kim Sablon, Principal Director for Trusted AI and Autonomy within the Pentagon's R&E Directorate, noted that the concept was designed to "bring the test and evaluation community with the research and development community together, to really start thinking through what the standard method process is for even providing evidence for assurance, and for measuring and calibrating trust along a human-system balance of roles and responsibilities.". The establishment of the centre comes at a crucial time in DoD's efforts to develop and adopt AI-enabled systems across a broader range of activities. For example, in August Deputy Secretary of Defense Kathleen Hicks announced the start of the [Replicator program](#) that seeks to create thousands of small, attritable, and expendable autonomous uncrewed systems in the next two years to counter the size and scale of China's on-going military modernization. This ambition is laudable. However, [an Atlantic Council report](#) on battlefield applications of human-machine teaming released in August argues that DoD efforts to adopt AI-enabled systems—both autonomous robots and decision-support tools—has been slowed by organizational, cultural, and bureaucratic issues. It has also been negatively affected by a lack of trust between operators and AI partners that the new DoD centre is designed to address.

2 Autonomous systems and robots

2.1	**Australian cardboard drones used in Ukrainian attack on Russian airfield**
	Australia has been sending 100 Corvo drones to Ukraine per month since March. ([source](#) and [source](#))
	Assessment: In late August, Ukrainian forces launched a swarm of single use Corvo drones carrying 4 – 5kg explosives to strike a Russian airbase in Kursk, about 100 km inside Russia's border. The strike was notable for the reported damage inflicted—a MiG-29 and four Su-30 fighter jets were damaged as were missile launchers and an S-300 air defence system. But it was also notable for the innovative nature of the Corvo drone, specifically that it is made almost entirely of waxed cardboard and rubber bands. This design approach greatly reduces not only the system's cost—each Corvo is reported to cost only USD3,500—but also its radar signature and airframe weight down, increasing its range. Australian company SYPAQ developed the drones using funding from the Australian Army Defence Innovation Hub, and the Australian government has shipped 100 systems to Ukraine per month since March 2023.
	The effective use of such a low-tech solution against some of the most advanced equipment in the Russian military's arsenal is worth noting as another example of how the creative design and use of low-tech capabilities can create significant asymmetric threats to much more expensive and advanced equipment. Consider the use of improvised explosive devices during the war in Iraq, in particular, which had a significant effect on the US. military's ability to carry out operations and led to resources being spent on developing a new class of vehicle with greatly enhanced protection. As advanced technologies such as AI / ML, directed energy, and others are increasingly incorporated into military capabilities, defence and security communities will certainly need to develop operational concepts for their use. They will also need to build systems (such as Red Teaming) to understand the asymmetric tactics and capabilities less sophisticated militaries or non-state actors might seek to employ to abrogate technological advantages.

Figure 2: An image from August 2020 of the SYPAQ cardboard drone similar to the one used in the Ukrainian attack on a Russian airbase. Source: SYPAQ company website

2.2	**Airwars and Der Spiegel profile Russia's use of Iranian drones**
	The in-depth piece examines how Russia has used the Iranian Shaheed-136 and Shaheed-131 in its invasion of Ukraine. ([source](#))

Assessment: On 8 September, Airwars, in conjunction with Der Spiegel, published a multi-media in-depth analysis entitled *A Year of Shaheed: How Iranian Drones Became a Key Tool in Russia's Arsenal.* The piece traces how Russia has incorporated the Shaheed-136 and Shaheed-131 since they were first documented in Ukraine in September of 2022 and determining that "while the Shaheed first emerged as part of the Russian arsenal a year ago, the tempo and intensity of attacks across Ukraine has escalated significantly since spring 2023."

Much like SYPAQ's cardboard drones, the Shaheed kamikaze drones are not particularly technologically sophisticated, and their value lies in the comparative advantage of cost, clever concepts of operations, and simplicity. They are notoriously loud and slow and their lack of manoeuvrability in flight makes them as similar to a missile as to an autonomous aerial system. However, they are also relatively cheap, costing only $50,000 per system and have a range of up to 2,000 kms, providing a low-cost, long-range option for striking at critical civilian infrastructure far away from the front – line. Russia has most often deployed Shaheeds in barrages that fly at low altitudes (making them hard to detect via radar) and has used them to target Ukraine's energy and food infrastructure. The use of barrages increases the chances that more systems will penetrate Ukrainian air defences and forces Ukraine into "[expending] valuable ammunition shooting them down", according to Samuel Bendett, an expert on the Russian military at the Center for Naval Analysis.

Beyond the physical damage done, the article also emphasizes the psychological effect of a Shaheed drone barrage attack. As noted above, the systems are loud, generating a buzzing noise that alerts citizens and soldiers that they are approaching. One Ukrainian citizen quoted in the article relayed that "It's very difficult to convey. I won't say I had a panic attack, but first of all, I felt a certain helplessness on the one hand, that you can't do anything … The only thought is, "Oh God, when will it all be over, and I hope it doesn't fall here. In reality, you understand that it's a lottery, it's a big lottery, it can fall anywhere." Moscow has denied that it is importing Shaheeds, instead claiming the weapons are indigenously produced Geran-1 or Geran-2 drones, though, as the article points out, there is "clear evidence of their Iranian origins."
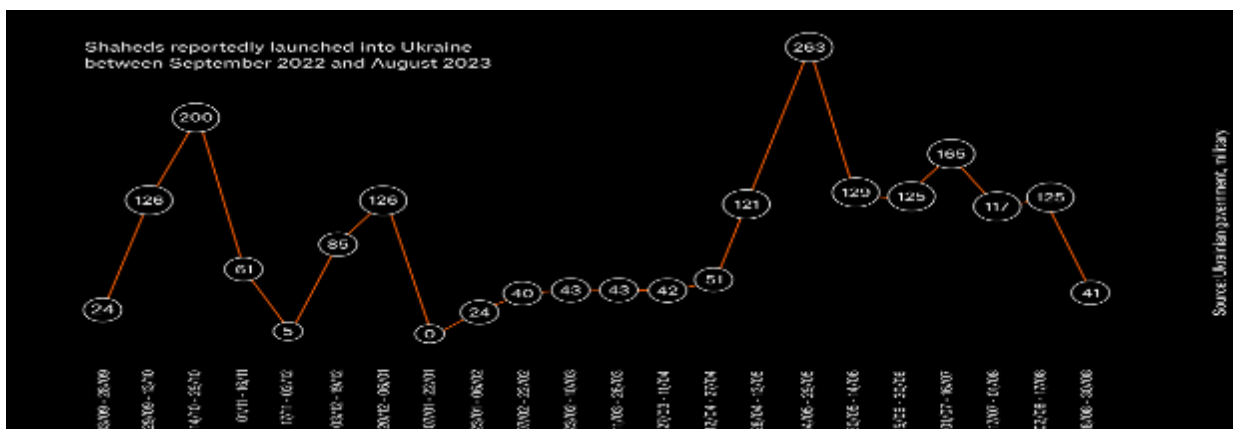

Figure 3: An Airwars produced chart depicting Russia's usage of Shaheed drones from September 2022 through August 2023. The extended dip in usage in early 2023 is largely due to supply chain issues that slowed delivery of Shaheed systems. [Source](#)

2.3	**An historic first: British drone flies to, lands on, and takes off from an aircraft carrier**
	Successful test signals advancement of a new model for naval aviation that more fully incorporates the use of autonomous uncrewed systems in conjunction with crewed planes and helicopters (source)
	Assessment: On 8 September, the UK Royal Navy reported that a W Autonomous System (WAS) drone flew from the Lizard Peninsula and landed on the deck of the HMS Prince of Wales aircraft carrier sailing off the Cornish coast. The uncrewed aircraft delivered symbolic supplies, and then took off from the aircraft carrier, returning to the location of its original departure. This demonstration marked the first time the Royal Navy had achieved this objective.
	The test was described as a "vital step" in the progression of Royal Navy carrier aviation. The service seeks to use drones to reduce or even eliminate over time the need to launch Merlin and Wildcat helicopters to deliver supplies or mail to carriers at sea or carry out ship-to-ship flights, thereby reducing both cost and risk to humans of these operations. The use of drones in this "dull" mission will also ensure that the Royal Navy's Merlin and Wildcat helicopters are free to carry out operational sorties, including anti-submarine or anti-surface warfare reconnaissance.
	While the Royal Navy has experimented with small quad-copter drones in the past, the use of a larger fixed-wing autonomous aircraft that did not require a remote human pilot is a massive step forward. The WAS autonomous system can carry up to 100kg payload up to 1,000km and can land on uneven ground or a runway as short as 150m long (a little half the length of the UK's Queen Elizabeth-class carriers)

Figure 4: A photo of the autonomous system being collected after its successful landing on the HMS Prince of Wales. Source: UK Royal Navy

2.4	**A new concept for continual reconnaissance for combat vehicles**
	Teledyne FLIR revealed its Black Recon combat vehicle reconnaissance system concept at DSEI in London in September. The concept allows for autonomous launch and recovery of multiple drones from inside military vehicles. ([source](#))

Assessment: The centrepiece of the system concept is a new micro-drone that will fly ahead of a moving combat vehicle. Each system includes three of these drones. One drone is deployed at a time, and the system automatically launches a relieve and replace drone when it senses that the deployed drone's batteries are running low. Flight duration reportedly exceeds 45 minutes.

Ketil Vanebo, a Senior Director of International Business Development at Teledyne FLIR described the recovery system: "A cradle arm autonomously recovers [the returning drone] using patented technology to track, capture, and dock the system. Another one can then deploy, while the first recharges for the next mission." The drones are stored in a launch box that can be mounted to several types of combat vehicles.

An original vehicle recon system using FLIR Systems' Black Hornet – 3 micro-drone was trailed in 2018. However, the Black Hornet – 3 is designed for use by dismounted soldiers rather than for vehicle operations, making it a poor fit for the mission and leading to the development of a new small drone. The system is not yet operational, though the company claims it has had discussions with several potential customers. |

3. Manufacturing and Industry

3.1	**Japanese MoD invests in 3D printing**
	The Japanese Ground Self-Defence Force (JGSDF) agreed to partner with SPEE3D to introduce the company's WarpSPEE3D and XSPEE3D printers. ([source](#))
	Assessment: In September, the JGSDF announced it had awarded a contract to SPEE3D, a company that specializes in the use of cold spray additive manufacturing technologies for defence communities. As part of the contract, the JGSDF will receive a WarpSPEE3D and an XSPEE3D printer. WarpSPEE3D is SPEE3D's first large-format metal 3D printer – able to produce large metal parts quickly in minutes or hours, according to the company. The XSPEE3D offers a robust, deployable metal additive manufacturing capability with SPEE3D's patented cold spray 3D printing technology, and auxiliary equipment integrated within one containerized shipping container unit. Together, the systems will provide JGSDF a capacity to build metal parts on-site and on-demand. According to a video produced by the company, the cold spray method does not require lab-like conditions or dangerous chemicals to manufacture key parts. The company also advertises that its XSPEE3D printer—which was developed in conjunction with the Australian armed forces—can produce several defence-grade materials such as Aluminium 6061, Aluminium Bronze, Copper, and Stainless Stee.l

Figure 5: Top: The XSPEE3D printer. Source. Bottom: a 2kg aluminium-bronze gunner's ratchet that was produced in 60 minutes using the XSPEE3D system.

3.2	**NATO to boost arms production**

The communique from NATO's Vilnius summit in July describes the establishment of a Defence Production Action Plan intended to increase the efficiency and scale of munitions production across the alliance. ([source](#))

Assessment: The plan comes after nearly a year of discussions about how best to address the glaring challenge of munitions shortages that has been revealed by the Ukraine War. As Wendy Gilmour, NATO Assistant Secretary General for Defence Investment pointed out, "the firing rates [in Ukraine] were far beyond anything that had been anticipated", leading to stretched industrial bases in member states as many sought to increase support to Ukrainian forces.

The plan is divided into three "activity buckets":

1. Looking for efficiencies in the acquisition and delivery of defence equipment and supporting multi-national procurements;

2. Examining how to better match NATO's defence planning process with the production capabilities of individual states' defence industrial base. As part of this activity bucket, NATO will establish a "planning board" to facilitate discussion about industry capacity and supply chain risk;

3. Addressing challenges "inherent to defence industrial collaboration" across alliance member states, including contracting policies, intellectual property laws, and export control regimes.

The challenge of munitions production is not unique to NATO or to European states. Previous DEFTECH scans have highlighted the issue for Russia and the United States, among others. In fact, the United States' FY2024 National Defense Authorization Act (essentially, the bill that authorizes the funding of the DoD) currently under consideration by the US. Congress includes not only increased funding for munitions production but also a rare—and overdue—measure ensuring multi-year procurement for five types of long-range precision munitions thought to be crucial to future US efforts to deter conflict.

NATO's challenge is complicated, of course, by the need to coordinate and balance the separate priorities, capacities, and interests of 31 member states that may not fully align, particularly as it regards a valuable sovereign and strategic asset such as defence industrial capability.

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

deftech
defencefuturetechnologies

3.3	**Into the wild blue digital yonder: US Air Force chases the elusive digital engineering revolution**
	The US Air Force has been aggressive in its efforts to adopt digital engineering in the design and testing of advanced, cutting-edge platforms with mixed results. The on-going Next Generation Air Dominance (NGAD) program offers an opportunity to try a more balanced approach to adoption. ([source](#))
	Assessment: A 30 August *Defense News* report provided a useful overview for the challenges the US Air Force has experienced in integrated digital engineering into key programs and how these experiences will inform its use in the on-going development of the Air Force's NGAD program. While the article focused on US Air Force experiences and efforts, many of the insights about the advantages and limitations of digital engineering are relevant to small and large militaries around the world considering increased use of digital engineering approaches.
	The purported benefits of digital engineering are 1) it can drive down costs associated with the design and testing of advanced systems, allowing the majority of testing to be run in the digital domain through thousands or more of AI-enabled simulations instead of requiring the building of iterative prototypes to test in the real world; 2) The use of digital twins can enhance manufacturing and tooling efficiency by improving design and parts fabrication to the point where they fit together without shims; and 3) when incorporated alongside open architectures and modular designs, digital engineering can accelerate the ability to integrate new technologies into existing platforms or systems.
	However, the US Air Force experience in its incorporation efforts has been mixed. While there certainly have been successes, there has also been frustration with the limitations of the technology in its current stage of development and use as well. As Secretary of the Air Force Frank Kendall noted "it's a significant improvement, but it has been overhyped. More integrated digital designs, better modelling all help, but they're not revolutionary… They don't replace testing entirely." The T-7 program, for example, made early gains in design and testing at the start of the program but has been significantly delayed by issues with the ejection seat and with aerodynamic stability in certain conditions. While these challenges were not due to the use of digital engineering, digital engineering did not help identify them during the design and testing phase either.
	Still, the approach will be used in the design, testing, and manufacture of the critical NGAD program. Indeed, the aircraft's new adaptive engine is being designed using digital engineering, though stakeholders have learned from previous efforts and are incorporating real world test data gained through a previous effort to develop an adaptive engine for the F-35.As the NGAD program progresses between now and the end of the decade, it will be worth militaries around the world watching how and how successfully the Air Force is able to integrate digital world and real world testing and development efforts.

4   Connectivity

4.1	**"Infamous Chisel" strikes Ukrainian soldier's phones**
	Russian group Sandworm launched a malware campaign against the Android devices used by Ukrainian soldiers ([source](), [source](), and [report]())
	Assessment: A 31 August report from the US Cybersecurity and Infrastructure Security Agency as well as other law enforcement and national security organizations in the United States and other Five Eyes countries reveals that Sandworm, a group with ties to the Russian GRU's Main Centre for Special Technologies GTsST, launched a malware attack against Ukrainian forces designed to steal sensitive information from the battlefield. The malware, known as "Infamous Chisel ", infected user Android devices, periodically scanning them for sensitive files and network information for exfiltration. Ukraine's security agency discovered the attack earlier in August and had successfully "exposed and blocked" attempts by Sandworm to continue to gain access to Ukrainian networks. The report provides technical details of the malware and assesses that:
	1. the malware was of low to medium sophistication
	2. It was developed with little regard to defence evasion or concealment of malicious activity."
	A Ukrainian investigation determined that Russia was able to launch the malware attack after capturing Ukrainian computer tablets on the battlefield.

4.2	**US DoD releases new Cyber Strategy**
	The document is the organization's first new Cyber Strategy since 2018. ([source]() and [document]())
	Assessment: On 12 September, the US DoD released an unclassified summary of its newest Cyber Strategy. Key take-aways from the summary include:
	1. The need to develop technologies that can confound malicious actors and prevent them from achieving their objectives in and through cyberspace, including Zero Trust architectures, advanced endpoint monitoring capabilities, tailored data collection strategies, enhanced cyber forensics, automated data analytics, and systems that enable network automation.
	2. The need to work more closely with the defence industrial base and other private sector organizations that retain expertise and analytical capabilities to identify cyber threats and mitigate vulnerabilities on a global scale. The document also references "expanding public-private partnerships" to ensure DoD expertise is made available to support key private sector initiatives.
	In comments during the announcement of the release of the summary, Mieke Eoyang, Deputy Assistant Secretary of Defense for Cyber Policy, discussed lessons about the cyber domain learned from assessment of the war in Ukraine. Deputy Assistant Secretary Eoyang observed that cyber operations have been frequently employed but that they had a limited impact when used as an isolated tool and are much more effective and disruptive when integrated "in and alongside other warfighting capabilities."

5   Human Performance Enhancement and Protection

| 5.1	**Ukraine develops its own invisibility cloak**
	The garment is expected to reduce ability of Russian forces to detect thermal signatures of forward deployed Ukrainian snipers and special operations forces.(source and source)
	Assessment: Mykhailo Federov, Deputy Prime Minister for Innovation and Minister of Digital Transformation for Ukraine, announced in early October that Ukrainian scientists and engineers had developed an invisibility cloak like "in fairy tales." The cloak reportedly blocks the radiation of heat and "makes fighters invisible to the enemy." Ukrainian armed forces have already tested the cloaks and they are now available for mass production, according to a member of the team developing the cloak. The program was developed through the Brave1 research program, which was established as a pathway for start-ups and non-traditional defence suppliers to provide technology-enabled capabilities to support Ukraine's efforts to resist the February 2022 Russian invasion of Ukraine.
	Federov released a video of the cloak in action via X (formerly Twitter) on 4 October (screenshot below). In the video, two Ukrainian forces not wearing the cloak are clearly identifiable by thermal imaging optics. A third soldier is mostly concealed by the cloak, though the thermal imaging does pick up the individual's face and upper chest. The partial detection of the third individual was apparently the result of the soldier not wearing the accompanying protective mask and special glasses. If the whole system is worn it is expected to "blind a thermal imager", in Federov's words.
	Production capacity is limited to 150 units per month. In addition, while the cloak has successfully blocked thermal signatures, those wearing it must move slowly to realize the cloaking benefits. Running, for instance, will create additional thermal signatures the cloak may not mask. As a result of these two constraints, the initial value of the cloaks will be in enhancing the safety of special forces, reconnaissance, sabotage, sapper, snipers, and sentries, allowing them to observe enemy motions or wait for enemies to approach without being detected. .
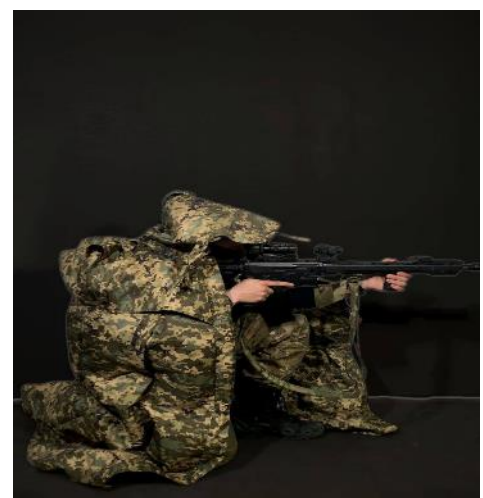
Figure 6: A screenshot from the thermal imaging video released by Federov on 4 October. Federov also released an image of the cloak being worn by a sniper. source

5.2	**Help from above: US investigating new role for uncrewed systems**
	US Army tests use of drones to support battlefield / disaster response triage ([source](#)—paywalled. [Additional source](#))
	Assessment: During the Northern Strike 2023 exercise held in Michigan, the US. Army used modified uncrewed aerial systems (UAS) to assess the vital signs of simulated injured / wounded soldiers on the ground. The drones were equipped with cameras and computer systems capable of identifying heart and respiration rates even though the simulated search and rescue mission took place 10 – 50 meters over forests and heavy brush areas. The test was part of the Army's Vision and Intelligence Systems for Medical Teaming Applications (VISTA) project. VISTA is designed to develop computer-vision-based software algorithms for injury detection and standoff vital sign monitoring that can be integrated into small drones for reconnaissance missions in hazardous areas. While the test was a success, the Army still seeks to develop a "more mature end-user device for the visualisation of medical information" collected by the drone to better allow a stand-off medic to triage a casualty scenario The Army is planning an additional test at a field exercise later in 2023.

6   New Weapons

6.1	**The third rail: Increased activity in rail gun development in the Indo-Pacific**
	Announcements from both Japan and China reflect continued interest in and progress for rail gun programs in the region. (source and source with additional background from source)
	Assessment: In September, *The South China Morning Post* (pay walled) reported that the People's Liberation Army (PLA) had developed a rail gun called the Gauss gun capable of firing a 124-kg projectile at a speed of 700 km / hour in less than .05 seconds, according to subsequent reporting from *The Defence Post*. On 16 October, Japan's Acquisition, Technology, and Logistics Agency (ATLA) announced that, along with the Japan Maritime Self-Defence Force (JMSDF), it had successfully tested a maritime rail gun for the first time. The two events reflect continued interest in the region in this interesting capability even as the United States has deprioritized development of these weapons.
	Rail guns use electrical power—rather than the chemical power used for the launch of traditional munitions—to fire projectiles at extremely high velocities, including hypersonic speeds. Rail gun projectiles do not contain explosives. Instead, they rely on the kinetic force to destroy targets at distance. Naval rail guns are conceived both as long-range strike and missile defence weapons (especially counter-hypersonic weapons), the latter of which is the key priority for JMSDF. The concept is not a new one—the French military first tried to develop the weapon in World War I—though technological advancements have made concept more realistic in the last decade -plus.
	However, as much promise as rail guns appear to hold, there have been persistent questions about their feasibility and utility in real-world operational environments, particularly in the maritime domain. The US. Navy spent 15 years and over $500 million attempting to develop a rail gun for its destroyers but abandoned the project in 2021 to dedicate more funds to hypersonic and directed energy weapons. In addition to the desire to reallocate funds to more mature technologies, there were also concerns about the viability of naval rail guns for two reasons. First, rail guns use electrical power that will need to be produced by the ship itself creating knock-on effects for ship design and power generation and storage. Second, rail gun launches are violent processes that wear down gun barrels quickly, reducing reliability and requiring a heavy back-end maintenance cost.

Figure 7: A screenshot from a video posted on ATLA's X account that shows the successful test of the maritime rail gun in October 2023. source: ATLA's X account

6.2	**"Frankenboat": North Korea reveals heavily modified "tactical nuclear submarine"**
	The boat is a dramatic rework of the Soviet Cold War Romeo-class diesel submarine and constitutes an initial step forward for North Korean efforts to develop a second strike nuclear deterrent capability. ([source](#) and [source](#))
	Assessment: On 6 September, North Korea revealed a new diesel-powered submarine capable of carrying multiple types of nuclear missiles during a ceremony at Sinpo submarine yard. The new vessel is named _Hero Kim Kun Ok_ and carries the hull number 841. The submarine is a heavily reworked and modified _Romeo_-class submarine that contains ten missile tubes of different sizes. The four at the front of the boat are larger and are likely to hold longer-range nuclear armed ballistic missiles, such as the Pukguksong family of submarine launched ballistic missiles. The rear six hatches are smaller and could house either smaller, shorter-ranged ballistic missiles or cruise missiles, such as the Hwasal-2 cruise missile, which is similar to the U.S Navy's Tomahawk missile.
	The unique boat appears to be the first step in a more extensive effort to develop a robust second-strike nuclear deterrent. In comments to NKNews, Kim Jung Un, outlined "a plan to remodel existing medium-sized submarines into offensive ones loaded with tactical nuclear weapons to play an important role in modern warfare." He also stated that this effort is a "low-cost ultra-modernization strategy."
	While the boat has been revealed, observers were sceptical that the ship on display constituted an actual imminently achievable operational capability, given the extensive reworking of such an antiquated submarine. Many expect the boat to undergo extensive testing and trials, including, most notably, testing to determine if it can launch submarine launched ballistic missiles.

Figure 8: Top: A screenshot from an Associated Press YouTube video of the submarine at dock during the ceremony. Bottom: A screenshot of Kim Jung Un in attendance during the ceremony from DW News' YouTube channel

7 Space

7.1	**Blue Origin announces plans for orbital transfer vehicle**

Details about the Blue Ring vehicle are scare—including any timelines for development—but the company does acknowledge an effort to develop a platform that could perform multiple services in space ([source](#))

Assessment: On 16 October, commercial space company Blue Origin announced it was developing the Blue Ring spacecraft, which it described as a "platform focused on providing in-space logistics and delivery" from medium Earth orbit to cislunar space (the part of space between the Earth and Moon) and beyond. Paul Ebertz, Senior Vice President of Blue Origin's In-Space Systems division said that "Blue Ring addresses two of the most difficult challenges in spaceflight today: growing space infrastructure and increasing mobility on orbit."

As more actors, both commercial and government, including defence and security organizations, seek to place more assets in and across more orbits, the need for affordable in-space infrastructure to support these satellites and spacecraft has expanded. Blue Ring is one of several solutions under development designed to fill various elements of this gap in existing capability. According to a graphic developed by Blue Origin executive Erika Wagner for an October 2022 presentation at the US National Academies committee meeting, Blue Ring is designed to deliver the services listed below across low Earth Orbit (LEO), medium Earth Orbit (MEO), geosynchronous orbit (GEO), in cislunar space, and in support of spacecraft traveling to other planets:

- Ride share
- Hosted payloads
- Communication relay
- Data storage and compute
- Refuelling
- Robotics platform
- In space assembly

The spacecraft will be able to carry payloads in excess of 3,000kg. Blue Origin has mentioned its intention to develop an orbital transfer vehicle capability in the past, including during two events in October of 2022. In its announcement, the company gave no indication of when Blue Ring will be operational. |

7.2	**German government blocks Chinese take-over of satellite firm**
	The German cabinet refused to allow Shanghai Spacecom Satellite Technology to acquire an additional 45% stake in German company KLEO Connect which is attempting to build a LEO communications constellation. ([source](#))
	Assessment: Shanghai Spacecom Satellite Technology already owned a majority share of 53% of KLEO Connect and was seeking to acquire the 45% minority stake held by German company EightyLeo. The government's decision to forbid the transaction was rooted in a growing concern about Chinese ownership of strategic assets, such as space-based communications architectures, which has also played out in discussions over Huawei's extensive control of 5G communications networks in Germany.
	KLEO Connect is one of several commercial companies globally that seeks to develop a constellation of hundreds of small, low earth orbit (LEO) communication satellites by 2028, similar to StarLink's LEO architecture only smaller. The decision is not a huge surprise, given the strategic importance of these constellations to military / national security activities, commercial activity, and civilian infrastructure. The near full Chinese ownership of a German company providing critical services to the German state and society does open up risks during a time in which Germany sensitivities to these risks have been heightened. In November 2022, for example, the government blocked possible Chinese investment in two German semiconductor producers due to national security and intellectual property concerns.
	Interestingly, [an aggressive and angrily worded statement](#) dated 26 September, 2003 from KLEO Connect's majority shareholders (Shanghai Spacecom) and posted on the KLEO Connect website rejects the strategic rationale for the government's decision. Instead, it deflects responsibility and charges that the decision is part of a broader conspiracy to "steal the KLEO Project and transfer it" to a German KLEO Connect competitor called Rivada Space Networks GmbH. According to the statement "a take-over of KLEO Connect GmbH has never been the objective of the Chinese majority investor." It also accuses EightyLeo and Rivada of "trying to take over the substantial investment of the Chinese majority shareholders in the German telecommunications joint venture."

8 Energy and Propulsion

<table>
<tr>
<td>8.1</td>
<td>

Propelling the youth: Australia seeks to build a pipeline of nuclear propulsion experts

The Australian government has launched a program to incentivize high-school students to study nuclear propulsion in submarines in a move designed to build the localized workforce to build AUKUS submarines in Australia over the next 12-plus years

Assessment: Australia's Department of Defence launched the Nuclear-Powered Submarine Propulsion Challenge in June 2023. The program seeks to inspire a next generation of nuclear submarine design talent to take advantage of the opportunities created by the Australia-UK-US (AUKUS) agreement to provide Australia with longer-range nuclear-powered submarines by 2035.It will provide teachers with resources to help students design their own nuclear-powered submarines, and winners will be invited to take place in "an immersive submariner experience at HMAS *Stirling*, the home base of Australia's Collins-class submarines."

Rear Admiral Jonathon Earley, the Deputy Chief of the Royal Australian Navy, offered that "the Nuclear-Powered Submarine Propulsion Challenge presents an opportunity for students across Australia to gain a greater appreciation of the STEM principles behind one of the most significant national projects ever undertaken in Australia (AUKUS submarine design and construction), as we prepare to deliver nuclear-powered submarines for the Royal Australian Navy."

The program highlights the importance of not only recruitment and retention of talent in the short-term but also the long-term investment in human capital development pipelines. This is especially the case as Australia and other militaries enter into an environment in which there is likely to be a shortage of qualified STEM graduates to support the range of technology development and integration programs that defence communities are pursuing.

</td>
</tr>
</table>

https://deftech.ch/