



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

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

# deftech.scan

## May 2022



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

<https://deftech.ch/scans>

**deftech**  
defencefuturetechnologies

Dear Reader,

If you are familiar with the deftech.scan, you will notice a new format compared to the one used during the last 2 years: less narrative and a new organisation in different technology areas.

Why that? The main reason is to better adapt to the changing environment, not only to the actuality, but also to the new topics covered by the evolution of [armasuisse Science and Technology](#) and to the evolution of the interaction with our various stakeholders.

Quicker to read, the new format should also be easier to translate using AI services. Last but not least, the classification into [technology areas](#) is an attempt to harmonize different collaborative foresight activities around those topics.

<b>1</b>	<b><i>Applications of AI and data</i></b>	<b>2</b>
<b>2</b>	<b><i>Connectivity</i></b>	<b>4</b>
<b>3</b>	<b><i>Autonomous systems and robots</i></b>	<b>6</b>
<b>4</b>	<b><i>Energy</i></b>	<b>7</b>
<b>5.</b>	<b><i>Human capacity enhancement</i></b>	<b>8</b>
<b>6.</b>	<b><i>Manufacturing and materials</i></b>	<b>10</b>
<b>7.</b>	<b><i>Sensors</i></b>	<b>11</b>
<b>8.</b>	<b><i>New weapons</i></b>	<b>13</b>
<b>9.</b>	<b><i>Space</i></b>	<b>15</b>

If foresight is about the future, we are true believers that the best way to start looking for it, is in the present!

We wish you an interesting read.

Foresightly Yours,



Tate Nurkin  
OTH Intelligence Group  
CEO  
[tate.nurkin@othintel.com](mailto:tate.nurkin@othintel.com)



Dr. Quentin Ladetto  
armasuisse S+T  
Head of Technology Foresight  
[quentin.ladetto@armasuisse.ch](mailto:quentin.ladetto@armasuisse.ch)

## 1 Applications of AI and data

<p>1.1</p>	<p><b>The promise and peril of AI development in synthetic biology</b></p> <p>A March 2022 paper in <i>Nature</i> detailed the results of an experiment in which US-based company Collaborative Pharmaceuticals altered their proprietary machine learning drug discovery tool to prioritize toxicity instead of penalizing it. The result was the synthetic generation of 40,000 dangerous molecules in six hours. The paper is based on a presentation delivered at a conference hosted by the Swiss Federal Institute for NBC Protection—Spiez Laboratory (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> The paper provides a useful “wake-up call” for the AI in drug discovery community (among other research communities that intersect with military and security endeavours) about the ease with which AI in conjunction with other technologies, in this case synthetic biology, being developed for salutary purposes can be easily and quickly altered to create weapons. A main amplifier of the risk of malign use of AI is the accessibility of the tools that could be used to develop or alter AI algorithms. The authors note that the company’s proprietary “underlying generative software is built on, and similar to, other open-source software that is readily available.” The paper also serves as a useful reminder that while AI’s implications for international security are a preoccupation for militaries, they are a blind spot for many commercial AI developers, potentially opening opportunities for defence community engagement on proliferation risks and considerations with dual-use industries. As the authors somewhat surprisingly and admirably confess, “When we think of drug discovery, we normally do not consider technology misuse potential.”</p>
<p>1.2</p>	<p><b>Synthetic data helps identify objects from space</b></p> <p>The use of synthetic training data to train AI algorithms to identify specific or rare items in satellite imagery—such as types of missile launchers or submarines—or common systems in unusual environments absent human review was a popular discussion area during the GEOINT Symposium held in the US in late April (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> As more intelligence, surveillance, and reconnaissance (ISR) assets and commercial earth observation / geospatial intelligence satellites are placed in space, the ability to rapidly and accurately discern items will be crucial to the effective exploitation of satellite imagery. Currently, though, computer vision models can struggle with rare items for which they have little training data. The result is that human subject matter experts must be called in to identify these items, slowing down the processing of images. Training computer vision models on synthetic data—data generated in a digital rather than real-world environment—offers a possible work around to this issue and the current limitations associated with AI-processed imagery. During the GEOINT 2022 Symposium in the US, several companies displayed synthetic data generation solutions, and the topic featured prominently in symposium panels. For example, L3Harris demonstrated how it creates synthetic imagery of fighter jets against different backgrounds and in various conditions and scenarios. Among the challenges associated with synthetic data use are ensuring accuracy and also reducing the vulnerability of synthetic data to adversarial data corruption efforts that could negatively affect or corrupt the training of AI algorithms.</p>

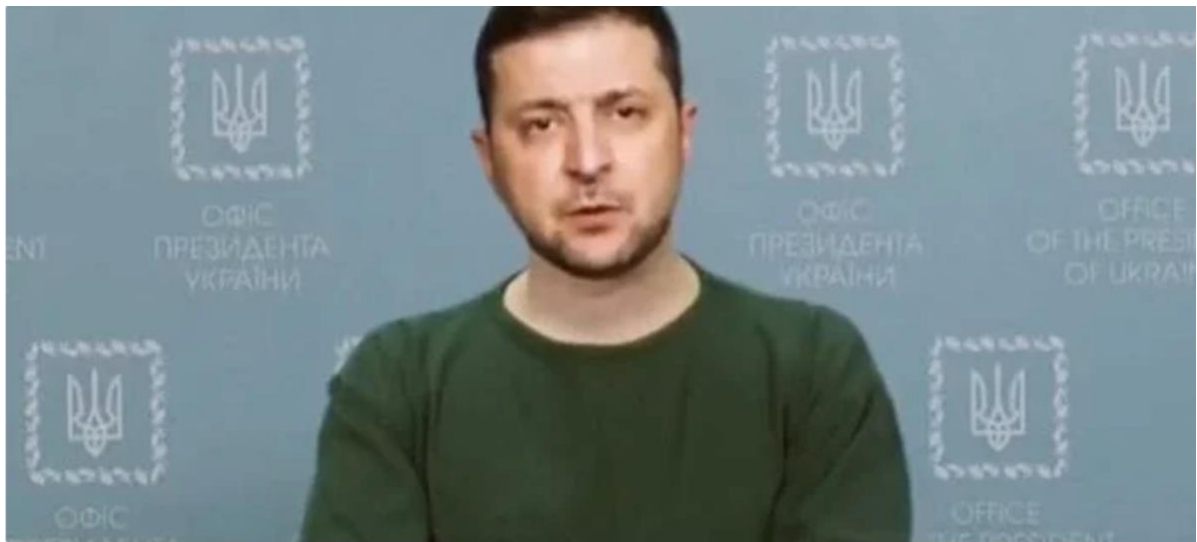
### 1.3

#### Zelensky deepfake draws rapid response and concern

A deepfaked video depicting Ukrainian president Volodymyr Zelensky appearing to tell Ukrainian forces to lay down their weapons and surrender to Russian forces appeared online in March. The deepfake was easily detected and quickly rebutted by Zelensky as well as other Ukrainian government sources ([source](#)).

**Assessment:** The deepfaked video was not a high-quality synthetic media. Mounir Ibrahim, vice president of impact at Truepic, a company established to detect deepfakes noted that “[the fact that it’s so poorly done is a bit of a headscratcher. You can clearly see the difference. This is not the best deepfake we’ve seen.](#)”

Nonetheless, the event elicited a strong response from Ukraine’s Centre for Strategic Communications and Information Security, which released a statement saying “Be aware—this is a fake! His goal is to disorient, sow panic, disbelieve citizens and incite our troops to retreat. Rest assured—Ukraine will not capitulate.” Analysts have noted that the Ukrainian response was aided by the fact that the government was prepared for the use of deepfakes, limiting the amount of time the video could spread without being debunked. Despite the poor quality of the synthetic media and effective Ukrainian of the response, the use of this deepfake has given analysts and observers pause about the future use of more sophisticated deepfakes that could find wider traction. The outcome of the prominent use of even moderately sophisticated deepfakes could “desensitize people and allow bad actors to allege ‘nothing is real on the ground; you can’t trust anything.’”



@MikaelThalen/Twitter

Figure 1: A screenshot from the original deepfaked video of President Zelensky. Source: @mikaelThalen (Twitter)



## 2 Connectivity

2.1	<p><b>US military to blend electronic warfare (EW) with cyber capabilities</b></p> <p>The US Navy's Next Generation Jammer will fly on the EA-18 Growler and be capable of both advanced jamming operations as well as RF-enabled cyber operations, continuing an on-going trend of the blending of EW and cyber activities (<a href="#">source</a>).</p> <p><i><b>Assessment:</b></i> Part of the impetus for the blending of EW and cyber capabilities stems from efforts by some states—particularly Russia and China—to place their military systems on wired networks that are firewalled from the internet, reducing the access points to and cyber-vulnerability of these systems. According to Bryan Clark a Senior Fellow at the Hudson Institute, “there’s a lot of interest in identifying new and innovative ways to get into opponents’ networks like the radar systems that’s being used to feed information into their combat system or an electronic warfare jammer aperture.” The Navy’s jammer is also expected to increase the range and ability to focus jamming capabilities through narrower beams on specific targets rather than merely blasting out jamming signals in a “megaphone”-like fashion.</p>
2.2	<p><b>SpaceX shuts down Russian EW attack in Ukraine</b></p> <p>In March, commercial space company SpaceX was able to shut down an attempted Russian EW attack against its Starlink satellite network, which was keeping the country of Ukraine connected to the internet during the on-going conflict. Senior US military personnel offered praise for the speed with which the private company was able to effectively respond to the jamming effort (<a href="#">source</a>).</p> <p><i><b>Assessment:</b></i> In early March, Russian forces were effectively jamming SpaceX satellites “for hours at a time.” In response, the company quickly updated its software code to meet the threat, immediately shut down the attacks. US Air Force Brigadier General Tad Clark called the rapid response “eyewatering” and observed that the US Department of Defense was not organized to achieve such agility. Indeed, a DoD response to these types of attacks would involve days of understanding the nature of the threats, fashioning responses, and deploying solutions, during which the functionality of affected satellites would be severely degraded. This disparity between the agile, risk tolerant approaches of commercial companies and more deliberate defence and national security communities is one that has been frequently highlighted in DEFTECH scans. The ability of defence and security communities to leverage commercial companies and their models for response will only gain salience in domains such as space and cyber marked by 1) a blurring of commercial, civilian government, and explicitly national security interests and activities; 2) increased national security-related competition; and 3) increased defence and security reliance on commercial assets and infrastructure.</p>

## 2.3

### Ukraine doxing Russian soldiers and spies

In March and April, Ukraine's intelligence services published the names and personal information of over 1,600 soldiers who served in Bucha, the site of a Russian military action that many in Ukraine and outside have suggested involved war crimes, and the names and contact details of 625 Russian intelligence agents ([source](#)).

**Assessment:** The Ukrainian government's "doxing" of Russian soldiers and spies constitutes a new phase in the intense and on-going information war that is helping to shape not only the situation on the ground in Ukraine, but also public perceptions of the conflict internationally. It is also a significant development in defence and security community efforts to exploit personal data and information of military personnel enabled not only by hacking, but also by the clever collection and curation of open-source personal information available through social media and other sources. While some argue that the personalization of psychological warfare / information operations constitutes a minor threat in comparison to the threat of violent death or bodily harm that is inherent in military operations, the psychology of conflict can be complicated. As Jessica Brandt, a fellow at the Brookings Institution's Center for Security, Strategy, and Technology observed, "the purpose of that activity is to highlight the costs to the Russian population at home and to impose costs on individual actors."

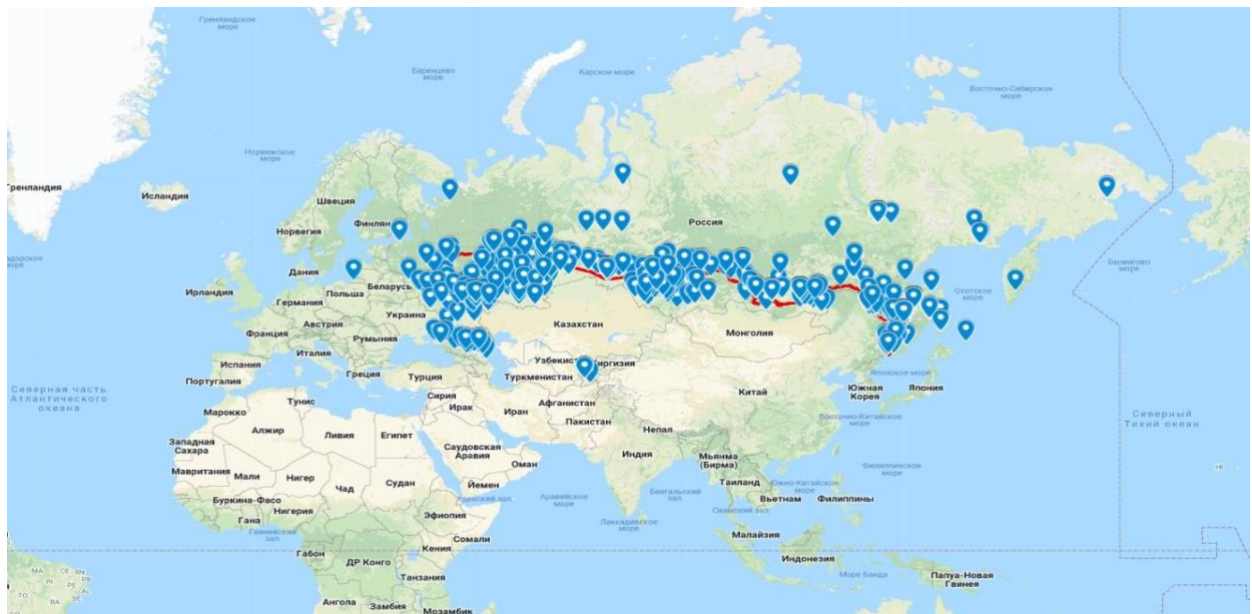


Figure 2: An image showing the hometowns of Russian soldiers that served in Bucha. The image is reflective of the personal data that the Ukrainian government has released regarding Russian soldiers over the last several weeks, including both open-source information and information acquired through cyber-espionage. Source: Odessa Journal

### 3 Autonomous systems and robots

<p><b>3.1</b></p>	<p><b>French Ministry of Defence (MoD) releases seabed strategy document</b></p> <p>French MoD released a strategy for increasing undersea operations at a depth of up to 6,000 meters. The strategy prominently highlighted the need to develop more advanced undersea autonomous and remotely piloted vehicles (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> The new strategy reflects the growing importance of the undersea domain generally to national security and defence communities as well as the intensifying competition to explore, map, mine, and protect the seabed. According to French Minister of Defence Francis Parly, “the emergence of drones and remotely operated robots—driven by the needs of industry [and] capable of carrying out operations that meet military objectives at a depth of several thousand meters—are transforming the seabed into a new space of strategic competition. “Of immediate interest outside of traditional military tasks is the ability to protect France’s undersea cables. In addition, many countries are increasingly looking to the seabed as a location to be mined for rare earths and other important minerals. The French strategy focused on both autonomous and remotely operated uncrewed vehicles (AUVs and ROVs) with the expectation that one AUV model and one ROV model will be developed by 2023 to serve as initial surveillance assets. The future anti-mine warfare system SLAM-F being co-developed with the UK as the Maritime Mine Counter Measures (MMCM) program (and featured in previous DEFTECH scans) is also part of France’s seabed strategy as is an effort to replace France’s three hydrographic vessels with more efficient and accurate capabilities.</p>
<p><b>3.2</b></p>	<p><b>Release the hounds: US Army exercise features drone swarms that operate like a wolfpack</b></p> <p>In April, the US Army announced that it plans to experiment with drone swarms that behave like a wolf pack at the aviation-focused Edge 22 exercise later this year (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> The move to a swarm approach that mimics a wolf pack is significant because, at least within parts of the US Army, it constitutes a shift away from the more commonly trialled approach of swarms that behave like insects. MG Wally Rugen noted in an interview with <i>Defense News</i> that in a wolf pack “there’s an alpha that kind of runs the show and then each wolf has a duty, but then those duties are hierarchical. And if one wolf gets knocked out by the antlers, a second one’s going” to step in. The test is expected to detect, identify, report, and geolocate threats, engage in electronic warfare and collaborative operations, navigate in a GPS-denied environment, and launch lethal effects, among other classified behaviours. While the shift from an “insect” based swarm to a “wolf pack” modelled one may seem subtle, it does serve as a useful reminder that as technologies around autonomous vehicles and swarming develop so, too, will the operational concepts for their deployment and use, which, in turn, drive demands for new technologies.</p>

## 4 Energy

<p><b>4.1</b></p>	<p><b>French MoD approves project to promote low-carbon military bases</b></p> <p>Reporting from February revealed that the French MoD will fund a feasibility study examining concepts to enhance the resilience and viability of fossil free and low carbon military camps. The 'ENSSURE' project (ENergy Self-Sufficient RESilient military base) was conceptualised under the guidelines of the European Union's Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS) (<a href="#">source</a> and <a href="#">also</a>).</p> <p><u><b>Assessment:</b></u> ENSSURE will examine the feasibility of energy self-sufficiency for small to medium-sized permanent military bases through the use of renewable energy sources (RES), energy management and energy efficiency tools and methods. The project seeks to better understand means of delivering this self-sufficiency while retaining combat capacity, described by the project's fact sheet as "non-negotiable", and also understanding the implications of changes to base infrastructure, energy sources, and practices. According to the project fact sheet, the effort is wholistic and will focus on designing technical solutions and improved practices that will enable a) energy sobriety (i.e., not wasting energy), energy efficiency to cover reduced final needs, RES and storage, and the use of microgrids and EMS. While interesting on its own merits, the project also reflects a growing effort by defence and security communities around the world to establish and contribute to net-zero carbon emission efforts.</p>
<p><b>4.2</b></p>	<p><b>Researchers develop material that could fundamentally change solar power</b></p> <p>Researchers at Imperial College London and City University Hong Kong have developed a new material that will reduce the cost and time associated with making solar panels (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> Traditional solar cells are made from silicon, which is expensive to make and can only be manufactured in still panels. The material perovskite can also be used to make solar cells. Perovskite solar cells can be printed from ink and therefore are lower cost, have high efficiency, are thin and lightweight, and flexible. However, to date they have not been durable, breaking down under normal environmental conditions. City University of Hong Kong researchers have now added ferrocenes made at Imperial College into perovskite solar cells, vastly improving their efficiency and stability. City University team tests and others done in commercial labs demonstrate that the efficiency of perovskite devices with an added ferrocene layer can reach 25%, approaching the efficiency of traditional silicon cells and passing the stability test set by the International Electrotechnical Commission, but at considerably less cost than silicon. More work is required to refine the material, but the City University team hope to bring the solution to market. Such a solution could offer promise for defence and security communities as they seek to reduce carbon emissions at bases and move toward carbon neutral activities.</p>



## 5. Human capacity enhancement

<p><b>5.1</b></p>	<p><b>Red 6 secures first export contract for virtual / real world air training system—blurring the lines between the real and virtual worlds as well as commercial and military activity</b></p> <p>Aviation training company Red 6 agreed to export its Advanced Tactical Augmented Reality System (ATARS) to the Kingdom of Saudi Arabia (KSA). The agreement also includes provisions for transfer of technology from Red 6 to KSA's Advanced Electronics Company (AEC) (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> Red 6's AI-enabled augmented reality technology allows for real-world pilots to train against or with virtual AI generated aircraft that are displayed through the ATARS headset. This ability to blur virtual and real-world training adds fidelity to the training process while greatly reducing costs, especially of adversarial air training. The US Air Force has previously awarded Red 6 a contract to integrate ATARS into the T-38 trainer aircraft. In addition to the increasing demand for more sophisticated training solutions that incorporate the virtual world, the deal is also notable due to the apparent agreement to share elements of Red 6's technology with AEC and the continued intersection between commercial and military technology areas. Frequently, this intersection involves militaries leveraging technologies developed for commercial purposes, though in this case KSA representatives have noted the relevance of the real world / virtual world training technology for "commercial applications in the Kingdom."</p>
<p><b>5.2</b></p>	<p><b>Portable desalination unit opens up opportunities for defence and security</b></p> <p>Researchers at the Massachusetts Institute of Technology (MIT) have developed a suitcase sized, portable, electrically-powered desalination unit that weighs less than 20 kgs and can remove particles and salts to generate drinking water, eliminating the need for filters (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> The new technology uses electrical power to remove particles from drinking water and "automatically produces drinking water that exceeds World Health Organization quality standards." It can be purchased online for around \$USD50. Rather than filtering the water, the team's ion concentration polarization (ICP) process applies an electrical field to membranes placed above and below a channel of water. The membranes repel positively or negatively charged particles as they flow past. The charged particles are funnelled into a second stream of water that is eventually discharged. The process also uses electrodialysis to remove any remaining salt ions. The MIT team used machine learning to find the ideal combination of ICP and electrodialysis modules. A video explaining the technology featuring the founder of the ICP process references two scenarios with relevance to defence and security communities. First, it could be used by refugees fleeing natural disasters (or other ills, such as conflict) supporting military humanitarian and disaster relief operations and, potentially, reducing conflict over drinkable water. Second, the video also notes that the technology is especially well-suited to support soldiers carrying out long-term military operations.</p>

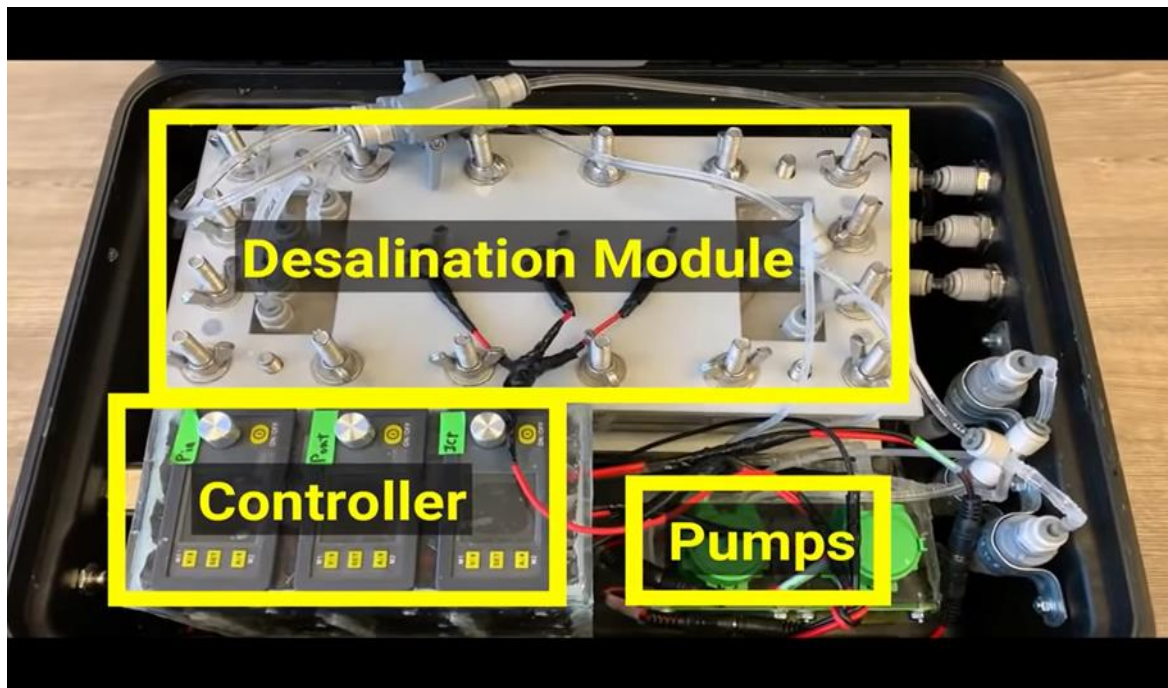


Figure 3: A screenshot of a video explaining the utility and functionality of the ICP water desalination system, which is a suitcase-sized device that is portable and can be operated with the push of a button. Source: [From seawater to drinking water, with the push of a button | MIT News | Massachusetts Institute of Technology](#)

## 6. Manufacturing and materials

<p><b>6.1</b></p>	<p><b>Raytheon cannot manufacture Stinger missiles fast enough</b></p> <p>Supplies of the US-manufactured Stinger missile have decreased since February when the US began shipping the lightweight, shoulder-launched air defence weapon to Ukraine. Concern over Stinger production rates reflect a broader challenge in replenishing munitions stocks during times of conflict (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> The Stinger missile has been an effective weapon for Ukrainian forces in the own on-going conflict with Russia. The US has shipped 1,400 Stinger missiles to Ukraine since the start of the war while other countries such as Lithuania have also provided Stingers. Lithuanian defence minister Arvydas Anusauskas posted in April that Lithuanian-provided Stingers had shot down at least six targets, though the claim has not been independently verified. However, Raytheon, Stinger’s manufacturer, has told the US government that stocks of the missile are dwindling, and the company has “a very limited stock of material for Stinger production.” Moreover, some of the components for the system, which the US DoD has not ordered in nearly two decades, are no longer commercially available, further complicating the task of increasing the production rate of Stingers, both to provide to allied and partner nations and to maintain a reserve for US forces. The issues facing Stinger production are not unique to this system or to Raytheon. The challenge of munitions production especially during wartime when munitions stocks are diminished through use are systemic and shared across nations and munition types. In addition to the supply chain challenges, the demand for munitions is typically conflict driven, and many companies are wary of creating spare capacity to develop systems for which there will be limited or only short-term increases in demand. While the munitions production challenge is complex and layered, some emerging technologies and manufacturing approaches can contribute to reducing the production dilemma. The increased incorporation of digital engineering can speed up design, testing, and upgrades of systems while the use of advanced manufacturing techniques such as additive manufacturing can reduce cost and timelines associated with scaling production. For example, <a href="#">a 2020 DARPA funded report from ASTRO America</a> advocated for a new approach to hypersonic missile development that heavily incorporated additive manufacturing to be able to make thousands of scramjet engines quickly.</p>
-------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 7. Sensors

7.1	<p><b>Australian company NIOA trials I-Rail small arms sensor-fusion technology</b></p> <p>Australian defence prime NIOA announced in March that it will trial a smart rail system that transforms rifles into real-time data nodes, linking soldiers in the battlefield with tactical leaders and commanders (<a href="#">source</a>).</p> <p><i><b>Assessment:</b></i> Australian defence prime NIOA is working with US company T-Worx to investigate application of its Intelligent-Rail (I-Rail) technology for use in the Australian Defence Force (ADF). According to NIOA, I-Rail will provide ADF forces with a fully integrated sensor platform with a single source of power and connectivity between weapon ancillaries including sensors. The system captures information from sensors on the weapon to create a data package that can include video, radio communication, ammunition usage, and location logistics. I-Rail was originally developed with funding from the US Army and is also in service as the basis for the NATO-powered Rail STANAG 4740/AEP-90. The decision to trial the I-Rail is driven by the growing appreciation for the increasingly data-centric nature of modern kinetic conflict. Pervasive sensors are providing soldiers with an abundance of information that can improve situational awareness, but only if this information is effectively processed and fused and usable to soldiers in the field.</p>
7.2	<p><b>A new Large Phased Array Radar is spotted in China, pointing toward Japan</b></p> <p>A satellite photo has revealed that China has built a new long-range, early-warning radar that can be used to detect ballistic missiles from thousands of miles away, likely giving it coverage of all of Japan (<a href="#">source</a>).</p> <p><i><b>Assessment:</b></i> A February 2022 satellite photo indicated that China has placed a new large phased array radar (LPR) at an existing mountaintop site in Yiyuan County, Shandong Province. The LPR is pointed in a north-easterly direction and was built sometime after November 2019. The LPR can potentially give China early warning of ballistic missile launches from North and South Korea, most of Japan, and even parts of Russia's Far East. The exact capabilities of the LPR are unknown, but China has invested in multi-layered and multi-dimensional sensing and early warning missile defence and space-tracking capabilities in order to provide maximum response time in a changing strategic environment. Specifically, Japan's increasing concern over China's boundary pushing behaviours and persistent territorial claims in the East China Sea have led to increased defence spending in Japan. It has also led to growing discussion within the Japanese MoD of developing a "counter-strike" capability in which Japanese forces would be allowed to strike forces in another country to support the defence of Japan's territorial sovereignty during a conflict. A robust Japanese counter-strike capability would be another significant change in Japan's defence position, which has been moving away from its long-standing and tightly interpreted defensive posture. China's early warning system also includes a growing number of space-based sensors and a network of over-the-horizon radars according to <i>Defense News</i>.</p>



## Large Phased Array Radar (LPAR) site, Yiyuan County, Shandong Province, China

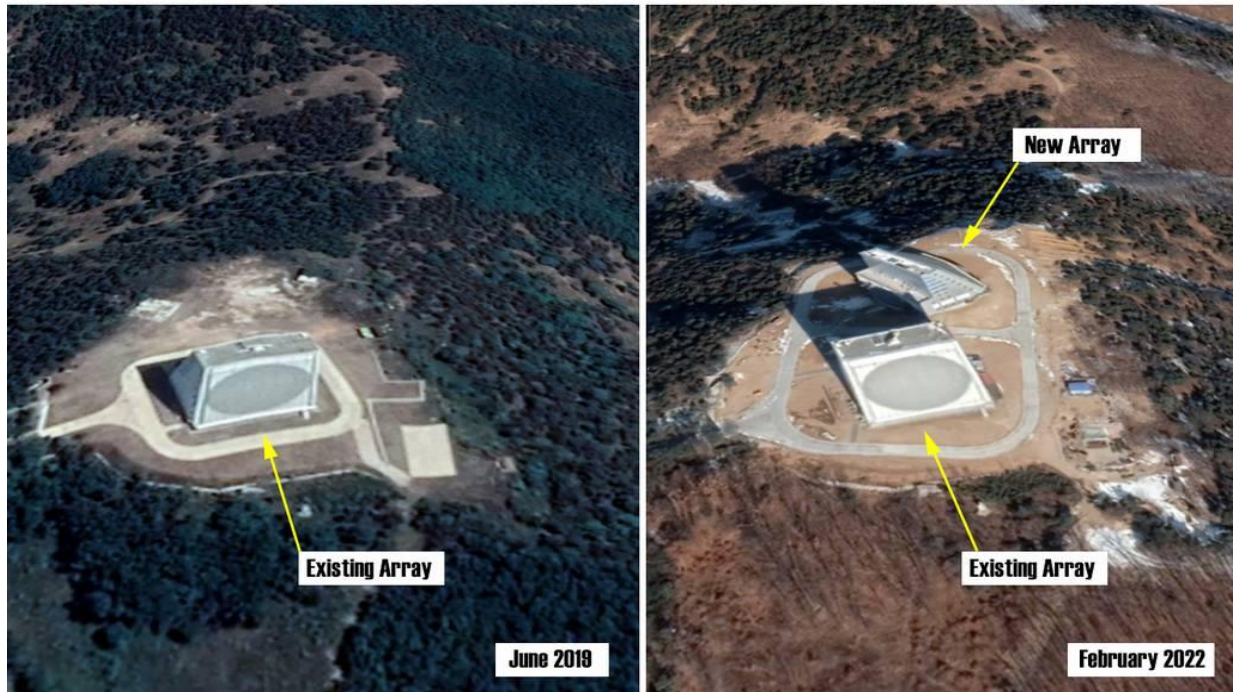


Figure 4: Satellite imagery of the LPAR site in Shandong Province China. The image on the right includes the new LPAR. Source: Maxar Technologies/Google Earth, via Defense News.

### 7.3

#### The unconventional war in Ukraine drives an unconventional response: Russia using trained dolphins to protect base at Sebastopol

Satellite images show that Russia is using trained dolphins to help defend the country's Black Sea naval base at Sevastopol. Russia / the Soviet Union have had a history of using marine mammals for base defence and mine detection in the past. ([source](#))

**Assessment** : Satellite images taken by Planet Skywatch reveal that the Russian Navy has placed two dolphin pens at the entrance to Sevastopol harbour, sheltered just inside a sea wall. The pens were moved there in February in advance of the start of the Ukraine conflict. The dolphins are likely to have been deployed to act as a sort of low-tech sensor to detect asymmetric and unconventional undersea threats such as individual or small groups of divers seeking to harm Russian warships in the harbour. While there has been no reported Ukrainian activity of this kind around Sevastopol, it seems increasingly clear that Ukraine is engaging in effective unconventional operations against Russian infrastructure in Russia. For example, [17 people were killed in a fire at a Russian research institute 100 miles outside of Moscow in late April](#), one of several fires and explosions at strategic sites around Russia since the beginning of the war. This is not the first time Russia / the Soviet Union have used trained marine mammals. The *US Naval Institute News* reports that the Soviet Union began training dolphins in 1991 and that marine mammals were deployed with Russian forces in the Black Sea in the 2014 Crimea operation while beluga whales pens have been established at a Russian naval base in the Arctic.

## 8. New weapons

8.1	<p><b>Russia tests Sarmat intercontinental ballistic missile</b></p> <p>Russia successfully tested its Sarmat intercontinental ballistic missile in April, according to comments from Russian President Vladimir Putin. (<a href="#">source</a>).</p> <p><u><b>Assessment</b></u> : The Sarmat –known as the Satan II in the West--is a next generation ICBM system that poses new and difficult challenges for integrated missile defence systems. It has a short boost phase, meaning that opponent's air defence systems will have a shorter period of time to find and fix the missile (and potential interdict in the boost phase) reducing their capacity to track the system as well. The Sarmat is also capable of carrying 10 warheads and / or decoys, raising the risks that missile defence systems could become saturated, overwhelmed, or unable to strike real targets via the launch of even one Sarmat missile fully loaded with warheads. The timing of the launch is also significant, given that both current challenges facing Russian forces and weaponry in Ukraine to date and the upcoming 9 May Russian Victory Day parade. The successful test launch allows the Russian government to highlight a significant military-technological achievement during the parade even as Russian forces have struggled to gain and hold territory in Ukraine. Observers also believe that the test was designed to deter perceived military escalation from NATO nations by demonstrating what the Russian Ministry of Defence referred to as “the most powerful missile with the longest range of destruction of targets in the world.”</p>
8.2	<p><b>Russia claims first use of hypersonic missile in combat, testing and development continue among US and its allies</b></p> <p>Russia claimed it has become the first nation to use an air-launched hypersonic missile during the conflict in Ukraine in March. The Kinzhal missile was reportedly employed to strike an underground arms depot in western Ukraine (<a href="#">source</a>).</p> <p><u><b>Assessment</b></u>: While the reported first use of a hypersonic strike system does constitute an important milestone, most commentators and observers have stressed that the Kinzhal's use in combat does not constitute a game-changing capability for Russia in the Ukraine conflict or potential future conflicts. The Kinzhal, like the Sarmat, is billed as one of Russia's “invincible” weapons systems, however it is thought to be an Iskander missile modified to be launched from a fighter jet. While it does constitute an upgrade in capability, concerns remain both about its accuracy and about how many of these systems Russia has left to launch. The Ukrainian MoD announced in March that Russia had fired almost all of its Iskander missiles in the first 20 days of the conflict. The Kinzhal's launch was not the only hypersonic strike system news during the reporting period. The United States Defense Advanced Research Projects Agency (DARPA) and US Air Force <a href="#">conducted a successful test of its Hypersonic Air-breathing Weapon Concept (HAWC) in March</a>, though the Department of Defense avoided announcing the test for two weeks in an effort to avoid inflaming tensions with Russia. The test took place only days after the Kinzhal launch and involved the HAWC demonstrator flying at speeds past Mach 5 and at altitudes higher than 65'000 feet (20 km), and for more than 300 miles. In addition, on April 5, <a href="#">US President Joe Biden and Australian Prime Minister Scott Morrison announced</a> that the United States, United Kingdom, and Australia are expanding the AUKUS security pact to include the co-development of hypersonic strike systems, further reinforcing the increasing significance of these weapons..</p>

### 8.3

#### Israeli air defence system intercepts mortar, US also has successful electric laser test

Israel tested a laser weapon system that successfully knocked drones, mortars, and rockets out of the sky in what a senior Israeli officer called a “game-changer” for ground-based airborne defence ([source](#) and [also](#)).

**Assessment:** Israel announced on 14 April that the Ministry of Defence and defence company Rafael had successfully tested the “Iron Beam” laser air defence system against three tiers of low-flying threats: uncrewed aerial vehicles (UAVs), rockets, and mortars. Israeli Prime Minister Neftali Bennett said in a tweet that the system had brought down the cost of intercepting these threats to \$3.50 per shot, a figure that does not incorporate the sunk costs of developing the system. Nonetheless, this is considerably less than the hundreds of thousands of dollars per shot of the Iron Dome kinetic interceptors. Israel has pushed development of laser systems as part of a broader layered air and missile defence system that can protect the country from rocket and mortar launches as well as from Iranian UAVs. As with hypersonic weapons, the Israeli test was not the only notable laser weapons system development during the reporting period. The US Navy successfully shot down a target drone replicating a subsonic cruise missile with a fully electric laser for the first time. The February test featured Lockheed Martin’s Layered Laser Defense (LLD) system, which disabled the engine on the drone. As with the Israeli test, the US test was designed to demonstrate how lasers can provide a critical layer of air and missile defence against several types of incoming threats.

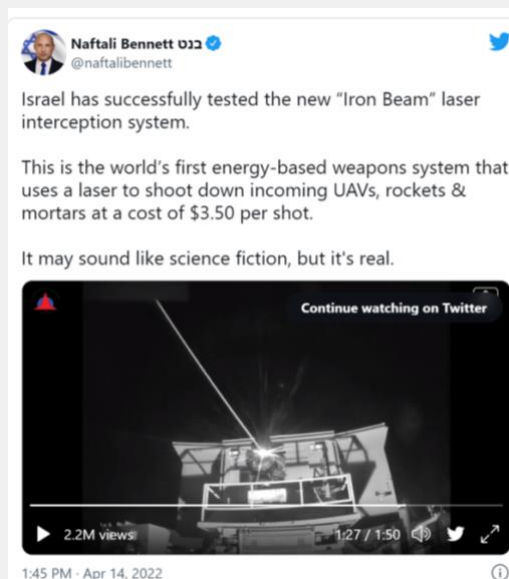


Figure 5: A screenshot of the tweet from Prime Minister Bennett announcing the successful test that also included a video of the system shooting down each tier of threat. Source: Neftali Bennett Twitter

## 9. Space

9.1	<p><b>Canada to establish space division</b></p> <p>Canada's military will establish a new space division later this year as it further develops its capabilities and skills for space operators (<a href="#">source</a>).</p> <p><u><b>Assessment:</b></u> Canada becomes the latest military to increase its focus on activities and competition in space by establishing a dedicated organization to produce the forces to be employed in operations across Canada's services. The current Canadian space enterprise has about 180 people, though the ambition is to grow the new division to approximately 270 people to include active-duty and civilian personnel. The organization will not have authority over space-related procurements, however. Comments from Royal Canadian Air Force Brigadier General Michael Adamson, the service's current director general for space, indicate that recruitment of space-focused talent, developing understanding what Canadian capabilities are required in space, and working with commercial space capability to meet requirements are all immediate focus areas for the nascent department, which is expected to be formally stood up in the next six to eight months.</p>
-----	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------





<https://deftech.ch/>