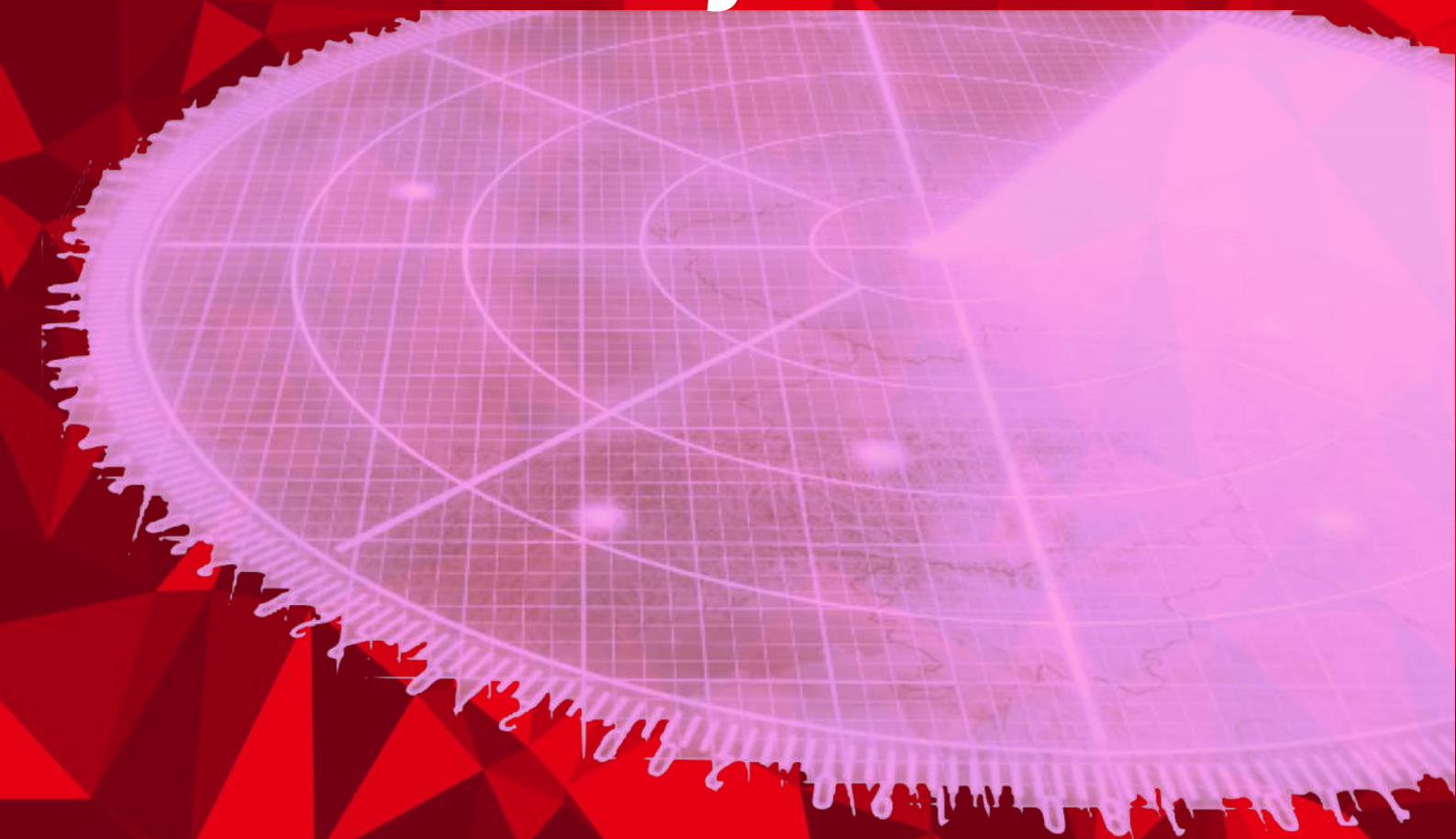
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Deftech Scan

June 2021



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

https://deftech.ch/scans

deftech
defencefuturetechnologies

Dear Reader,

While after almost 10 years of discussions, we are still debating about the potential use of LAWS (Lethal Autonomous Weapons Systems) on the battlefields and how to regulate them, the first generations of such products are making their coming out.

Considering the major focus on swarming and the progresses to be expected in human-machine interactions via augmented reality, pieces of our science fiction narratives are becoming tangible products at a pace that will always surprises us. Of course, these systems are not perfect, but we see that given the circumstances it might not be a necessary pre-requisite for some actors.

The same dynamic is also perceptible in different areas such as stealth, hypersonic propulsion and space, not to mention the cyberspace which has been quite a lot recently. With all these technological developments taking place simultaneously and that quickly, we can only wonder how long could an advantage based on technology last?

We wish you a nice reading

Foresightly Yours,

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

Dr. Quentin Ladetto
armasuisse S+T
Research director – Technology

quentin.ladetto@armasuisse.ch

Introduction and Executive Summary

This DEFTECH SCAN reports on and assesses occurrences in military technology and capability development taking place from late March through late May. It contains reporting on recent activities and announcements in the United States, United Kingdom, Germany, Estonia, France, Russia, China, South Korea, Israel, Turkey, and Australia. It also covers multiple NATO activities and includes general commentary on developments related to emerging capabilities such as cognitive electronic warfare and drone swarms.

As with the March volume—and all DEFTECH SCANS moving forward—where appropriate this report emphasises the intersection between defence and security activity and the coronavirus pandemic.

Resilience: More fundamentally, the report has a strong focus on how militaries and security communities are improving resilience against an expanding set of challenges. The emphasis on resilience cuts across most sections of this report, including descriptions and analysis of:

- An effort to build more rugged stealthy materials to optimize performance in harsh conditions
- The vulnerability to cyber-attacks of both industry and infrastructure in different countries and of the efforts to build resilience to these increasingly prevalent and damaging attacks
- Plans to build proliferated space architectures of small satellites in part designed to enhance resilience of crucial space-based capabilities

Other key themes and insights from the report include:

Key Events: The reporting period saw several significant events that demonstrate the role emerging defence technologies and activity in the cyber and space domain and the electromagnetic spectrum are playing in shaping the future of conflict and prioritised military capabilities. Four events stand out:

- The role of Israel's Iron Dome short-range missile defence system played in the 11-day Israel-Hamas conflict in May
- An increase in cyber-attacks against both industry and critical infrastructure, including a ransomware attack against oil pipelines in the United States that led to a run on gas across much of the East Coast of the U.S.
- The U.S. Army awarding a $22 billion dollar contract to Microsoft for 120,000 augmented reality headsets that will drive the technology forward for both military and commercial applications
- The release of UN report that confirmed the first known use of a lethal autonomous weapons system against humans during the conflict in Libya in 2020

Meeting Novel Threats: Enhancing Collaboration and Flexibility: This reporting period once again demonstrates the need for collaboration—between civilian government and militaries, between national governments, and between militaries and academia and industry—to meet the threats facing defence and security communities.

The reporting period also highlighted the emerging need for militaries to develop flexible and layered solutions that can reduce risk and ensure operational efficacy in different contexts and operational environments. For example, militaries are devising multiple new technologies and operational concepts to intercept small uncrewed aerial systems, including techniques designed to bring down these systems with little to no collateral damage in populated areas in addition to kinetic means of destroying drones. Similarly, multiple exercises in the reporting period demonstrated the mission flexibility of uncrewed ground vehicles (UGV) and the ability of some UGVs to serve in multiple supporting functions depending on the situation with only limited modifications.

Energy, Power, and Design

Key Insights:

- **New Technologies to Optimize Hypersonic Propulsion and Stealth:** Academic researchers have demonstrated new technologies that offer increased efficiencies related to two of the most important areas of the future of military aircraft propulsion and design. The demonstration of an oblique wave detonation engine offers promise for a stable propulsion system that can propel an aircraft to up to Mach 17 and offer an alternative to scramjets. Similarly, another research team demonstrated a new ceramic coating that will increase the resilience of stealth aircraft, enable more efficient designs, and increase their performance.
- **Update on Hybrid Engines:** Hybrid engine development has been a frequent topic of interest to DEFTECH SCANS, including the March edition which highlighted the growing and sustainable demand for hybrid systems in the aviation industry. According to reporting from *Shephard Media*, in May, the UK MoD revealed testing of new hybrid-electric drive (HED) prototype variants of the British Army's Jackal and Foxhound protected mobility vehicles has begun. The project to develop HED has moved quickly with contractor NP Aerospace delivering HED systems for the two vehicles within nine months, working closely with the vehicles' original manufacturers. NP Aerospace developed the HED using only existing technologies and off-the-shelf components that are already available. Testing will collect data on areas such as drivability, fuel economy, endurance, and reliability.

World First: Oblique Wave Detonation Engine: Researchers at the University of Central Florida (UCF) claim to have demonstrated an oblique wave detonation engine (OWDE) capable of propelling an aircraft up to 17 times the speed of sound.

Members of the research team had previously demonstrated the viability of a rotating detonation engine in 2020 "in which shockwaves from one detonation are tuned to trigger further detonations within a ring-shaped channel." However, the OWDE demonstration marks an important step forward for this technology area. The test produced a continuous detonation that is stable and fixed in space providing an even more efficient and controllable "propulsion system capable of generating significantly more power and using less fuel than current technology allows." [1]

The team built a prototype called the High-Enthalpy Hypersonic Reacting Facility or HyperReact, which is less than one meter long and is separated into three sections, as seen in the Figure 1 schematic below:

> *"This is the first time a detonation has been shown to be stabilized experimentally. We are finally able to hold the detonation in space in oblique detonation form. It's almost like freezing an intense explosion in physical space."-Kareem Ahmed, member of the UCF team*

Section One is a mixing chamber in which a pre-burner ignites a jet of hydrogen fuel that has been premixed with air and is accelerated to appropriate speeds by four more air channels around the pre-burner.

Section Two is a converging-diverging nozzle. The main fuel injector adds 99.99 percent ultra-high-purity hydrogen fuel to the hot, fast, high-pressure air coming in from the mixing chamber just before it enters the CD nozzle, which tapers down to a 9mm high "throat" before diverging back out to a 45-mm square again. The design enables the acceleration of the mix up to Mach 5.

[1] Loz Blain, "World first: Oblique wave detonation engine may unlock Mach 17 aircraft", *New Atlas,* May 12, 2021, World first: Oblique wave detonation engine may unlock Mach 17 aircraft (newatlas.com)

Section Three—the test section—is where the detonation takes place. This section takes the hypersonic air / fuel mix and runs it up a ramp with a 30-degree angle on the bottom side of the square tube.

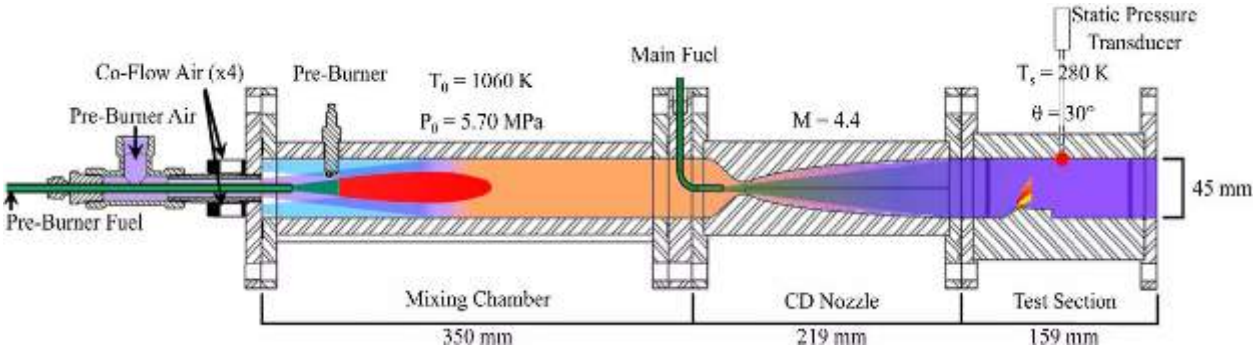


Figure 1: A schematic diagram of the experimental HyperReact prototype (Source: University of Central Florida via New Atlas)

The OWDE offers the potential for a more efficient and effective form of hypersonic propulsion to the scramjet engine, which is thought to top out at speeds around Mach 14 while the UCF experiment indicates an ability to propel aircraft or, plausibly, missiles at up to Mach 17.[2]

In November 2020, several Chinese researchers published an article in the *Chinese Journal of Aeronautics* that proposes a standing oblique detonation ramjet (Sodramjet) engine concept as an achievable means of working around the inefficiencies of scramjet engines at high hypersonic speeds. The article concludes, "the experimental data show that the Sodramjet engine model works steadily, and an oblique detonation can be made stationary in the engine combustor and is controllable. This research demonstrates the Sodramjet engine is a promising concept and can be operated stably with high thermal efficiency at hypersonic flow conditions.[3]

The Future of Stealthy Materials?[4] Researchers at North Carolina State University (NCSU) have developed a new ceramic material that could increase the resilience of stealthy aircraft to harsh conditions, abrasive materials, and extreme heat, potentially fundamentally altering the approaches to designing and developing stealth aircraft.

The polymers used to absorb radar signals on stealth aircraft are susceptible to degradation from salt, water, abrasive materials, and temperatures above 250 degrees Celsius. To cope with the challenges of extreme heat, fifth generation aircraft include design accommodations such as the nature of the wing design and inclusion of long, thick, and heavy nozzles at the back of the plane to protect the material from extremely hot jet exhaust. These accommodations can affect performance, making the aircraft slower, less fuel-efficient, and heavier.

The research team at NCSU has developed a ceramic coating designed to ruggedize stealth coatings and allow stealth aircraft to maintain their stealthiness in harsh conditions and for longer periods of time. The material is water resistant, harder than sand, more radar absorbent than stealthy polymers, and retains its stealthy properties at temperatures over 1,800 degrees Celsius.

The ceramic is applied by spraying a liquid ceramic precursor onto the surface of the aircraft. The precursor experiences a series of chemical reactions as it is exposed to air, ultimately converting it to a solid ceramic material after one or two days. Chengying "Cheryl" Xu, the leader of the research team, captured the possible impact that the material could have, assessing that "if we get the support we need to

[2] Ibid.
[3] Zonglin JIANG, Zijian ZHANG, Yunfeng LIU, Chun WANG, Changtong LUO, "Criteria for hypersonic airbreathing propulsion andits experimental verification", *Chinese Society of Aeronautics and Astronautics& Beihang UniversityChinese Journal of Aeronautics,* 28 November 2020, Criteria for hypersonic airbreathing propulsion and its experimental verification - ScienceDirect
[4] Matt Shipman, "How a tougher skin could change the shape of stealth aircraft", *NC State News,* May 18, 2021, How a Tougher Skin Could Change the Shape of Stealth Aircraft | NC State News (ncsu.edu)

scale this up, aircraft manufacturers will be able to fundamentally redesign stealth aircraft. . . The material we've engineered is not only more radar absorbent, it will also allow the next generation of stealth aircraft to be faster, more maneuverable and able to travel further."[5]

Human Performance Enhancement and Protection

Key Insights:

- **Militaries Pivoting to Meet Covid and Other Biological and Health Threats:** Militaries continue to dedicate resources to meeting the current challenge of the Covid-19 pandemic as well as to build resilience against future biological threats. These efforts have leaned on the scientific and technical expertise that many militaries can convene and support as well as the logistical capabilities, experience, and expertise of even small and mid-sized militaries.
- **Augmented Reality for Militaries Takes Another (Big) Step Toward Actual Reality:** The U.S. Army procured $22 billion worth of augmented reality headsets from Microsoft. And while the scale of this procurement is unlikely to be matched by other nations, particularly smaller militaries, the deal does reflect a growing interest of both small and large militaries in deepening development and integration of augmented reality not just for synthetic training, but also to enhance the situational awareness and target acquisition of personnel operating in increasingly complex, uncertain, and contested operational environments.

DARPA Moving Forward with Detecting Infections: The March 2021 DEFTECH SCAN detailed efforts of the U.S. Defense Advanced Research Projects Agency's (DARPA) establishment of the Nucleic acids On-demand Worldwide (NOW) program. The program is designed to develop a mobile medical countermeasure manufacturing platform that will rapidly produce therapeutics in days for deployed personnel.

Figure 2: 60 Minutes presenter Bill Whitaker holds a vial containing the sub-dermal sensor that can detect illness in an individual servicemember's blood before they show symptoms. Other reporting about the sensor reflected another growing challenge of Covid-- disinformation and misinformation—as several news organizations reported that DARPA was developing an implantable "microchip" to monitor individuals, leading to numerous and erroneous conspiracy theories on-line. Photo: 60 Minutes YouTube channel

On March 19, the agency published an extensive list of active programs to provide technical and scientific solutions to address the Covid-19 pandemic as well as other possible biological threats. The list includes thirteen programs separated into three main categories:[6] Diagnose & Detect; Treat & Prevent; and Manufacture.

DARPA's counter-Covid efforts gained particular attention during the reporting period due to a feature on U.S. news program *60 Minutes* that highlighted some of the agency's on-going work. Specifically, the program focused on an effort to develop a tissue-like "sub-dermal implant" that acts as a sensor continuously monitoring the state of an individual servicemember's blood, detecting infection before symptoms emerge.[7]

The sensor acts in the same way a "check engine" light in a car does. It alerts the individual of an irregularity—in this case, an infection—but does not necessarily identify exactly what infection has been detected. Military personnel that receive the signal would then self-administer a blood test to better

[5] Ibid.
[6] "The DARPA Difference: Pivoting to Address Covid", DARPA, March 19, COVID-19 (darpa.mil)
[7] "A sensor that can tell if you're sick", *60 Minutes YouTube channel,* 9 April 2021

understand what the infection is and what steps need to be taken not only to treat that individual but also to protect other personnel and stop the spread of diseases in the frequently close-quarters environments in which military personnel operate, such as ships.[8]

Germany's Bundeswehr Opens 24 / 7 Vaccination Clinic: On Easter, Germany opened its first always-open vaccination center in the state of Saarland. The facility is staffed and operated by 108 Bundeswehr soldiers from the medical service who are on duty to vaccinate people against the coronavirus in three shifts daily seven days a week.[9] The Bundeswehr has plans to open two more 24 / 7 facilities, and 3,000 Bundeswehr personnel are reportedly administering vaccines at various locations.[10]

The episode is just one indicator of the role that the German military—and militaries more broadly—have played in building not only resilience within their own ranks but also in their broader society and that of allies and partners, especially regarding the delivery of vaccines. For example, in February, the People's Liberation Army delivered vaccine doses to both the Pakistani and Cambodian militaries.[11]

Military Augmented Reality Becoming Actual Reality[12]: On 31 March, the United States Army announced it had awarded Microsoft a $21.9 billion contract to deliver 120,000 customized HoloLens headsets based on the Army's Integrated Visual Augmentation System (IVAS). Microsoft was previously awarded a two-year $480 million contract in 2018 to develop and test the bespoke AR system.

Figure 3: The Microsoft HoloLens headset developed for the U.S. Army. Source: Microsoft

The benefits of the headsets have been demonstrated during this prototyping and testing phase as an Army press release points out: "The suite of capabilities leverages existing high-resolution night, thermal, and Soldier-borne sensors integrated into a unified Heads Up Display to provide the improved situational awareness, target engagement, and informed decision-making necessary to achieve overmatch against current and future adversaries. The system also leverages augmented reality and machine learning to enable a life-like mixed reality training environment so the soldier can rehearse before engaging any adversaries."[13]

[8] Ibid.
[9] "Vaccination around the clock: 24-hour vaccination center of the Bundeswehr starts", *Bundeswehr website,* 4 April 2021, Vaccination around the clock: 24-hour vaccination center of the Bundeswehr starts
[10] Elisabeth Braw, "Germany's Military an Unexpected Star in Pandemic Relief", *Defense One,* 20 April 2021, Germany's Military an Unexpected Star in Pandemic Relief - Defense One
[11] Amber Wang, "Coronovirus: People's Liberation Army provides Covid-19 Vaccine to Pakistan Military", *South China Morning Post,* 7 February 2021, Coronavirus: People's Liberation Army provides Covid-19 vaccines to Pakistani military | South China Morning Post (scmp.com)
[12] Loz Blain, "Microsoft to build $22 billion worth of AR headset for US military" *The New Atlas,* 31 March 2021, Microsoft to build $22 billion worth of AR headsets for the US Army (newatlas.com)
[13] Ibid.

Cyber and C4ISTAR

Key Insights:

- **Cyber Conflict:** Cyber-security threats were at the forefront of defence and security activity during the reporting period. A suspected Chinese – government sponsored spear-phishing attack on one of Russia's largest submarine design companies demonstrated the scale of China's on-going efforts to acquire advanced military technology even through surreptitious means against one of its geopolitical and defence industrial partners. A significant ransomware attack against major gas pipelines in the U.S. led to runs on oil throughout the Southeastern United States, revealing the need for enhanced resilience measures in the face of the loss of critical infrastructure.
- **Creative and Collaborative Countermeasures:** As awareness of the cyber threat grows, more creative and, critically, collaborative means of countering this threat are being pursued by both large and small militaries. Indeed, NATO member states held a conference in Estonia to discuss the need for a common and coordinated cross-alliance approach not just to protecting military networks and assets, but to build increased social, political, and economic resilience to expanding cyber challenges. Multi-level collaboration with industry is also required, including the types of "adversarial collaboration" seen in the U.S. Department of Defense's (DoD) "bug bounty" program that encourages white hat hackers to find vulnerabilities in DoD systems.
- **Proliferated Architectures of Small Satellites:** In addition to the sharpening and urgent focus on cyber-security, many defence and security communities around the world are also considering new ways to develop more resiliency in the crucial and increasingly contested domain of space. The reporting period saw announcements from both the U.S. and UK that stressed the need to build architectures consisting of small satellites in Low Earth Orbit both to provide new or enhanced capabilities and to provide a measure of protection against growing counterspace capabilities

Subs, Pipelines, Exercises, & Bounties: The Cyber Threat in 2021: Cyber-security threats were at the forefront of defence and security activity during the reporting period, once again revealing the diversity of threat vectors challenging industry, military, and especially broader national and economic security resilience in countries around the world.

In early May, cyber-security firm Cybereason released a report documenting a cyber-attack against Russia's Rubin Design Bureau, one of the country's leading submarine manufacturers. The attack used an image file with malicious software embedded inside it via a "specific tool that has become a hallmark of multiple entities linked to the Chines government."[14] Rubin designs the ultra-quiet *Borei* class ballistic missile submarine, the *Belgorod and Losharik* special missions submarine, and the *Poseidon* nuclear powered, nuclear armed ultra-long range uncrewed underwater vehicle / torpedo.[15]

Cybereason first reported the attack on 30 April, though it is not clear exactly when the attack actually took place or whether or not it succeeded. The cyber-attackers emailed the file to Rubin's general director Igor Vladimiroich. The image file was a sophisticated rendering of an autonomous underwater vehicle that is nearly identical to a system under development by Rubin. Undersea systems expert H.I. Sutton noted that ""Whoever drew it knew a lot about AUVs and Rubin designs. So the image itself appears legit."[16]

[14] "PortDoor: New Chinese APT Backdoor Attack Targets Russian Defense Sector", Cybereason, 30 April 2021, PortDoor: New Chinese APT Backdoor Attack Targets Russian Defense Sector (cybereason.com)
[15] Joseph Trevithick, "Top Russian Submarine Design Bureau Hit By Cyber Attack With Chinese Characteristics", *The Drive*, 10 May 2021, Top Russian Submarine Design Bureau Hit By Cyber Attack With Chinese Characteristics (thedrive.com)
[16] Ibid.

The image was infected with the RoyalRoad program that embedded a separate file, winlog.wll, into the image. The subfile would then deploy the malware, called PortDoor, onto the computer when the file was opened.[17] Cybereason noted that Portdoor was a "previously undocumented backdoor" with the ability to "do reconnaissance, target profiling, delivery of additional payloads, privilege escalation, process manipulation, state detection antivirus evasion, one-byte XOR encryption, AES-encrypted data exfiltration and more."[18] While the attackers are not identified in the report, Cybereason asserted that there were strong clues pointing to an actor working with the Chinese government.

Figure 4: A copy of the image sent to the director of Rubin Design Bureau as part of the cyber-attack against the company. (Source: Cybereason)

Western governments have frequently accused China's government and state-owned enterprises of cyber-theft of personal data, defense industry design secrets, and other sensitive intellectual property. That the suspected Chinese cyber-attack was against Russia—a geopolitical partner—is an interesting development, especially considering that the two countries are currently jointly developing a non-nuclear submarine.[19] However, China's growing focus on building out its undersea fleet in order to better compete with the United States, Japan, Australia, and other actors in the undersea domain in the Indo-Pacific and is likely driving interest in better understanding the designs and technologies of the novel undersea vehicles, such Rubin's Poseidon autonomous underwater vehicle (AUV) and Harpischord large uncrewed underwater vehicle (UUV).[20]

Also during the reporting period, a major ransomware attack against energy company Colonial Pipeline in the United States revealed another way in which cyber operations can threaten national security and test the resilience of critical infrastructure and of the societies this infrastructure services.

The 7 May attack against Colonial, the company that runs the U.S.' largest fuel pipeline, ended up shutting down all four of the company's major pipelines that serve the Eastern and Southeastern U.S.

[17] Ibid.
[18] "PortDoor: New Chinese APT Backdoor Attack Targets Russian Defense Sector", Cybereason, 30 April 2021, PortDoor: New Chinese APT Backdoor Attack Targets Russian Defense Sector (cybereason.com)
[19] Joseph Trevithick, "Top Russian Submarine Design Bureau Hit By Cyber Attack With Chinese Characteristics", *The Drive*, 10 May 2021, Top Russian Submarine Design Bureau Hit By Cyber Attack With Chinese Characteristics (thedrive.com)
[20] Ibid.

Figure 5: A gas station in Charlotte, North Carolina on May 13, 2021, six days after the cyber-attack that led to the shutdown of the Colonial pipelines. The station had no available gas to sell (Source: Tate Nurkin)

Gas prices rose driving a run on gas that led to many gas stations in the Southeast running out of gas.[21] Nearly 70% of gas stations in North Carolina, over half in Virginia, and about half in South Carolina and Georgia ran out of fuel to sell. Around Washington, D.C., reportedly 73% of gas stations ran out of fuel.[22]

Colonial Pipeline reportedly paid a ransom of nearly $5 million to regain control of its systems and restarted operations on 12 May, five days after the attacks.[23] It took several more days for operations to return to full capacity. The U.S. government believed the attack emanated from Russia or Eastern Europe, though it did clarify that it did believe that the threat actors were criminal gangs unaffiliated with the Russian government. According to U.S. President Joe Biden, there was "strong reason to believe that the criminals who did the attack are living in Russia. That's where it came from."[24]

The cyber threat against infrastructure and military assets, networks, and systems stemming from nation states, criminal groups, and other non-state actors is (perhaps belatedly) becoming a growing preoccupation for defence and security communities around the world. In April, senior NATO officials held the virtual NATO Cyber Defense Pledge conference that brought together senior government and private sector officials to discuss the need for improvements in NATO's cyber posture. The conference was part of the broader alliance effort of

Pentagon Bug Bounty Program Expanded

Protecting military and defence networks and systems in the highly contested and highly creative cyber-threat environment described in this report will require not only collaboration between nations, but also collaboration between defence and security communities and industry / academia / the broader cyber-security community within a given state.

One creative approach can be seen in the 4 May U.S. DoD announcement that it will expand its "bug bounty" program to all publicly accessible information systems. The program allows authorized hackers to investigate and report cyber vulnerabilities in industrial control systems, Internet of Things devices, and other networks. The program began in 2016. In the nearly five years since, hackers have submitted more than 29,000 vulnerability reports, 70% of which were validated by DoD. Brett Goldstein, director of the Defense Digital Service hailed the expansion as "a testament to transforming the government's approach to security and leapfrogging the current state of technology within DoD."

Source: Justin Doubleday, "Pentagon expands bug bounty program to all publicly accessible systems", *Inside Defense,* May 5, 2021, Pentagon expands bug bounty program to all publicly accessible systems | InsideDefense.com

[21] Julia Ainsley and Kevin Collier, "Colonial Pipeline paid ransomware hackers $5 million, U.S. official says", *NBC News,* May 13, 2021, Colonial Pipeline paid ransomware hackers $5 million, U.S. official says (nbcnews.com)
[22] Center on National Security at Fordam Law, CNS Morning Brief, May 14, 2021, CNS Morning Brief: Colonial Pipeline Operational After Paying Hackers $5 Million (mailchi.mp)
[23] Julia Ainsley and Kevin Collier, "Colonial Pipeline paid ransomware hackers $5 million, U.S. official says", *NBC News,* May 13, 2021, Colonial Pipeline paid ransomware hackers $5 million, U.S. official says (nbcnews.com)
[24] Ibid.

hardening member nations against catastrophic disruptions; in other words, to build resilience in and across NATO member states.[25]

> *"Enhancing resilience and leveraging technology will be key to a strong alliance in a more competitive world."—NATO Deputy Secretary-General Mircea Geoana at the NATO Cyber Defence Pledge conference*

The event was hosted by Estonia, a nation recognized for its proactive and effective approach to cyber security. Estonian Prime Minister Kaja Kallas highlighting the ways in which the coronavirus pandemic has exacerbated the cyber threat to NATO states, noting that "malicious cyber activities" against NATO members had increased since the beginning of the pandemic as states, militaries, companies, and individuals came to rely even more on connectivity. Kallas also highlighted that "cyberspace is at the forefront of increased global competition" and urged democratic nations to "stand together against deviations from acceptable behavior."[26]

Cognitive Electronic Warfare Book Review:[27]Electronic warfare (EW) expert Dr. Thomas Withington published a review in Armada International of the recently released book "Cognitive Electronic Warfare: An Artificial Intelligence Approach" by Karen Haigh and Julia Andrusnko.

Cognitive EW is a frequently cited future capability, but one that is, in Dr. Withington's opinion, less well-understood. With that in mind, one of the main values of the book is to offer a digestible explanation of cognitive EW, defining it as a system that "perceives the environment, reasons about the situation, and acts to accomplish goals" and that it "learns from interaction with the environment providing situation assessment, decision-making, and learning capabilities."

The book has an optimistic take on the future of cognitive EW, arguing that it will come on-line in a piecemeal fashion—indeed, the authors point out that cognitive EW is already being incorporated into some electronic warfare planning efforts—even if there are challenges related to the data on which cognitive EW systems operate, among others. Ultimately, Withington offers that "this robust, thought-provoking book will become a standard text in this fast-emerging field."

Driving Space Resilience Through Proliferated Architectures: The March 2021 DEFTECH SCAN highlighted the continued development of counterspace threats to commercial, civil government, and military space-based architectures. These emerging counterspace capabilities are now instigating efforts to build and sustain new types of architectures, especially proliferated constellations of small satellites in Low Earth Orbit (LEO) that offer not only resilience to space-based architectures but also the flexibility required to meet increasingly fast-moving contingencies.

In a 14 May *C4ISRNet* interview, United Kingdom's Air Chief Marshall Mike Wigston, the head of the Royal Air Force, revealed the Ministry of Defence (MoD) seeks to build a new intelligence, surveillance, and reconnaissance satellite constellation of "responsive launched small satellites" in LEO that can be outfitted with multiple payloads. As a result, UK forces will have "the option of selecting the payloads, selecting the role and selecting the position of the satellites, and then launching them and getting them into operation in a very, very short decision action cycle." Wigston continued by stressing the speed and resilience this type of constellation can provide to the war fighter, observing that the proliferated network

[25] Sebastian Sprenger, "NATO to improve cyber defense in bid to boost alliance resilience", *C4ISRNet,* 15 April 2021, NATO to improve cyber defense in bid to boost alliance resilience (c4isrnet.com)
[26] Ibid.
[27] Dr. Thomas Withington, "Thinking Aloud", *Armada International,* 6 May 2021, a review in Armada International of the recently-released book *Cognitive Electronic Warfare: An Artificial Intelligence Approach*

will provide the "ability to respond to a crisis in a particular part of the world, or perhaps a requirement to add some resilience to another part of the space network."[28]

The interview comes after the March release of the UK MoD's Integrated Review, which called for a new intelligence, surveillance, and reconnaissance satellite constellation. It also comes shortly after the U.S. Space Development Agency announced in early February that it would release an RFP in August for the development of 150 small satellites to begin to populate the LEO-based Transport Layer of its ambitious seven-layer National Defense Space Architecture. The Transport Layer will end up consisting of 300-500 small satellites and be responsible for transporting data across the proliferated defense space architecture using free space laser communications.[29]

Crewed Platforms

Key Insights:

- **Republic of Korea joins 'Big Boys' of Fast Jets:** The Republic of Korea displayed the first prototype of its KF-21 aircraft (formerly KF-X). The 4.5 generation fighter was domestically designed and built and relies on a wide range of indigenously manufactured systems. The aircraft is expected to help modernize South Korea's ageing fighter jet fleet from 2028 and will likely be made available for export in the already crowded 4.5 generation fighter jet market.
- **British Armoured Vehicles:** The March 2021 DEFTECH SCAN included details of a UK Parliament report that concluded that the UK's armoured fighting vehicle capability was "deplorable." In May, the Ministry of Defence awarded a contract for the acquisition of 148 upgraded Challenger 3 main battle tanks that will include new high-speed ammunition designed to greatly increase the lethality of the UK's main battle tank capability.
- **The Future of the Tank:** In combination with the advancement of the joint French-German Eurotank program, this procurement signals that talk of the "end of the tank" that emerged after Azerbaijan's use of loitering munitions against Armenian armoured vehicles was cited as a critical factor in the outcome of the Nagorno-Karabakh war. Future tanks and armoured vehicles will require new technologies—such as increased digitisation and longer-range, faster munitions—and new operational concepts, but militaries continue to invest in the capability.

South Korea's Boramae Revealed: Korea Aerospace Industries (KAI) displayed the first prototype aircraft under development as part of the high-profile KF-X program. The program was launched six years ago and has become a lynchpin of the Republic of Korean's efforts to further develop its indigenous aerospace and defence industries.

The newly named KF-21 Boramae (a boramae is a bird of prey) is a twin-engine 4.5 generation indigenously designed and built aircraft that will replace the Republic of Korea Air Force's (ROKAF) F4D/E Phantom II and F5E/F Tiger II aircraft starting in 2028.[30]

South Korean president Moon Jae attended the scenario, announcing that "we've got our own supersonic fighter jet finally. We have opened a new era of self-defence and established a historic milestone for the development of the aviation industry."[31]

[28] Aaron Metha, "British Royal Air Force invests in space capabilities", *C4ISRNet,* 14 May 2021, British Royal Air Force invests in space capabilities (c4isrnet.com)
[29] Teresea Hitchens, "Operational Comms, Missile Tracking Sats up in 2024: SDA", *Breaking Defense,* 11 February 2021, Operational Comms, Missile Tracking Sats Up In 2024: SDA « Breaking Defense - Defense industry news, analysis and commentary
[30] Jr Ng, "KAI rolls out KF-21 Boramae combat aircraft prototype", *Asian Military Review,* 14 April 2021, KAI rolls out KF-21 Boramae combat aircraft prototype - Asian Military Review
[31] Gordon Arthur, "PREMIUM: South Korea joins the 'big boys' with rollout of KF-21", *Shephard Media,* 13 April 2021, PREMIUM: South Korea joins the 'big boys' with rollout of KF-21 - Air Warfare - Shephard Media

KAI is already building the second and third of six prototype aircraft. The first of these prototypes should achieve its maiden flight in July of 2022. Production is expected to begin in 2026. The ROKAF has committed to acquiring 40 by 2028 and another 80 by 2032.[32]

Figure 6: The KF-21 Boramae prototype. The Boramae will be equipped with a domestically made AESA radar as well as locally made electro-optical targeting pod, infrared search-and-track system, and electronic warfare self-protection system. Source: picture Asian Military Review. Content: Asian Military Review and Shephard Media

The aircraft is also expected to be made available for export and was developed in conjunction with Indonesia, which pledged to fund 20% of the KF-X program. Indonesia has fallen behind its commitments and has reneged on payments since January 2019. Jakarta has contributed only $201 million, which is less than 15% of what it committed to spend to date. South Korea is expected to spend $8 billion on the program from its inception in 2015 through the initial procurement in 2028.[33] While initial production aircraft will be optimised for an air-to-air mission, serial production aircraft will be multi-mission and be able to perform air-to-ground missions as well.[34]

British Armoured Vehicles: From 'Deplorable' to the 'Most Lethal in Europe': The UK Parliament released a scathing report on the state of the country's armoured vehicle fleet—to include its main battle tanks—in March that concluded that armoured fighting vehicle capability was "deplorable."[35]

The MoD seems to have taken at least one important step in meeting the challenge laid down by that report by awarding a £800 million contract with Rheinmetall BAE Systems Land (RBSL) to produce a fleet of 148 Challenger 3 main battle tanks. The MoD press release asserted that the award means the UK will now have the "most lethal tank in Europe" while Defence Secretary Ben Wallace said that the acquisition "represents a huge shift in the modernisation of [UK] land forces through the increased lethality of Challenger 3", which incorporates high-velocity ammunition with higher ranges.[36]

The Challenger 3 will use the existing chassis of the in-service Challenge 2 tanks, but will include a more powerful engine, a more advanced gun, and will be fully digitised to facilitate data sharing and multi-domain operations. In addition, while the UK currently operates 227 Challenger 2s only 148 will be upgraded as the Army reduces its size to meet commitments from March's Integrated Defence Review (IDR).[37]

The UK was also named as one of several countries thought to be part of a "wave" of new partners for the joint French-German Eurotank that will emerge after a planned conference in September on the

[32] Ibid. and Jr Ng, "KAI rolls out KF-21 Boramae combat aircraft prototype", *Asian Military Review,* 14 April 2021, KAI rolls out KF-21 Boramae combat aircraft prototype - Asian Military Review
[33] Gordon Arthur, "PREMIUM: South Korea joins the 'big boys' with rollout of KF-21", *Shephard Media,* 13 April 2021, PREMIUM: South Korea joins the 'big boys' with rollout of KF-21 - Air Warfare - Shephard Media
[34] Jr Ng, "KAI rolls out KF-21 Boramae combat aircraft prototype", *Asian Military Review,* 14 April 2021, KAI rolls out KF-21 Boramae combat aircraft prototype - Asian Military Review
[35] "Obsolescent and outgunned", U.K. Parliament Defence Committee, U.K. Parliament website, 14 March 2021, Obsolescent and outgunned: the British Army's armoured vehicle capability - Defence Committee - House of Commons (parliament.uk)
[36] "British Army to possess most lethal tank in Europe", *UK.Gov,* 7 May 2021, British Army to possess most lethal tank in Europe - GOV.UK (www.gov.uk)
[37] "British Army to get 148 Challenger 3 tanks in £800m deal", *BBC,* 7 May 2021, British Army to get 148 Challenger 3 tanks in £800m deal - BBC News

program. According to a "close-hold" document dated from March and obtained by *Defense News,* the event is being planned to catalyse an "opening wave" of interested countries from across Europe, assuming that France—which has been more reticent than Germany to expand the program to date—and Germany can agree on prerequisites for joining the program.[38]

Weapons Systems and Munitions

Key Insights:

- **Asymmetric and Unconventional Threats:** Militaries around the world are increasing focus on several emerging and rapidly evolving asymmetric and unconventional threats, especially the expanding missile threat, the counter small UAS (Unmanned Air Systems) mission, and other challenges such as sea mines. These threats are generating requirements for new capabilities that are, in some cases, enabled by emerging technologies and / or by creative operational concepts, such as the use of loitering munitions as a flying minefield for counter small UAS defence.
- **Right-Sizing Responses:** Meeting these new challenges is also pressing both small and large militaries to consider the appropriate scale of response for novel threats in various environments in order to control costs and ensure the most efficient response that produces the least collateral damage. For example, using expensive missile interceptors to cope with low flying and short-range rockets creates unsustainable cost curves and makes military and security communities more vulnerable to saturation attacks that overwhelm the ability to respond. Similarly, using non-kinetic means such as electrical pulses to destroy sea mines offers considerable cost and mission efficiency advantages over explosive ordnance. The use of non-kinetic means of intercepting small drones can reduce collateral damage in populated areas and urban environments.

Iron Dome and the Evolving Missile Threat: Israel successfully employed Rafael Advanced Defense Systems' Iron Dome missile defence system against short-range rockets fired by Hamas during the 11-day conflict.

Iron Dome is designed to detect and shoot down missiles and 155mm artillery shells fired from between four km and 70 km away. The system is based on Rafael's advanced ELTE ELM-2084 multi-mission radar (MMR). The system detects incoming fires, tracks their trajectory, and predicts where the missile will land. The battle management system uses this data to prioritise incoming munitions based on the scale of the damage individual fires are likely to cause on their current trajectories. Interceptor missiles are then fired to destroy the missiles in air before they reach their targets.[39] Each missile is estimated to cost about $50,000, a sum considerably less than many interceptor missiles used in advanced air and missile defence systems.[40]

[38] Sebastian Sprenger, "Germany expects 'wave' of new Eurotank partners after September conference", *Defense News,* 14 May 2021, Germany expects 'wave' of new Eurotank partners after September conference (defensenews.com)
[39] Andrew Drwiega, "Bunker Briefing-17 May 2021", *Armada International,* 17 May 2021, EDITOR'S BUNKER BRIEFING 17 MAY 2021 No.58 - Armada International
[40] Ibid.

There are reportedly 10 Iron Dome systems in use in Israel, each with three or four rocket launchers with 20 missiles for each launcher.[41] The system has been in existence since 2011 but was the subject of extensive coverage during the conflict, given its approximately 90% success rate in shooting down missiles launched from Gaza.[42] In addition, several arresting pictures taken of the system in action at night—such as the one taken by Anas Baba of AFP and featured below—were published during the conflict, further amplifying the discussion of Iron Dome's performance during the conflict.

Figure 7: Iron Dome interceptors (left) in action against rockets fired from Gaza (right). Source: Anas Baba, AFP

The evolving nature of the missile threat to states and military installations and assets was also at the centre of NATO's Exercise At-Sea / Formidable Shield, which began on 15 May and will run through 3 June off the Scottish Coast and Andova training site off Norway. The exercise will involve 15 ships and dozens of aircraft from Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, the UK, and the U.S. and will focus on working together "to defend NATO forces and populations from the very real threat of missiles," according to NATO spokesperson Piers Cazalet.[43] The exercise is particularly important in light of the fact that, again according to Cazalet, "missile arsenals [are] growing and becoming more complex" [44] to include high-end cruise and ballistic missiles, hypersonic missiles, loitering munitions, autonomous uncrewed aerial systems, and the sorts of short-range rockets that dominated the Hamas-Israel conflict.

> *"In conflicts around the world, cruise and ballistic missiles are often the weapon of choice, both for state and non-state actors. So at a time when we see missile arsenals growing and becoming more complex, it is important that Allies continue to adapt and exercise our defences."—NATO spokesperson Piers Cazalet*

The Counter-Drone Mission: As recognition of the expanding small drone threat increases, militaries around the world are pursuing creative solutions to match the layered nature of the small uncrewed aerial system (s-UAS) challenge.

[41] Uta Steinwehr, "Israel's Iron Dome proves successful against Gaza rockets", *Deutsche Welle,* 12 May 2021, Israel's Iron Dome proves successful against Gaza rockets
[42] Ibid.
[43] Andrew Drwiega, "Bunker Briefing-17 May 2021", *Armada International,* 17 May 2021, EDITOR'S BUNKER BRIEFING 17 MAY 2021 No.58 - Armada International
[44] Andrew Drwiega, "Bunker Briefing-17 May 2021", *Armada International,* 17 May 2021, EDITOR'S BUNKER BRIEFING 17 MAY 2021 No.58 - Armada International

Russian firm ZALA Aero Group, which was acquired by Kalashnikov Concern in 2015, is working to adapt its Lancet-3 (also sometimes referred to as the "Lantset-3") loitering munition to support the counter-drone mission as a drone interceptor. The operational concept involves a formation of Lancets patrolling the airspace above friendly troops ready to intercept any in-coming drones. ZALA claim that the Lancets could patrol for up to tens of hours, forming an aerial minefield. Achieving this level of coverage would require ZALA either to develop greatly enhanced endurance for the Lancet-3 as its battery currently allows only forty minutes of operations before it needs to be recharged *or* for the operational concept to include frequent rotation of Lancet-3s in and out of the aerial minefield on a regular basis.[45]

> *"A major challenge [for security forces] is the homegrown terrorist, a lone wolf actor who decides that drone technology is something they can use to inflict fear without putting themselves at risk. [Another] challenge is the prospect that in wartime, our military forces will be confronted with a very sophisticated swarming drone capability. Australia needs to be able to defend against that threat in order to preserve our capability." – Dr. Malcolm Davis, Australian Strategic Policy Institute in comments to SBSNews published in an article by Sandra Fullon published on 14 May 2021*

In April, the U.S. Army and Joint Counter UAV Office (JCO) held demonstrations of three low collateral effects counter-drone interceptors, reflecting the complexity of the small UAS threat and the need for layered responses. The Army's concern is that while kinetic destruction of threatening drones may be appropriate in some operational contexts, there are other environments such as in populated areas in which is a pressing need to reduce collateral damage. The Army demonstrated three systems as reflected in the figure below:[46]

Figure 8: The three systems demonstrated during the US Army's low collateral effects interceptors demonstration in April 2021. Source: Tate Nurkin, The UAS Threat and Approaches to Countering It, briefing delivered on 29 April 2021 at Ft. Campbell,

Non-Kinetic Counter-Mine Solutions: Two novel approaches to coping with the growing challenge of maritime mines were demonstrated during the reporting period. Reporting from 30 April noted that the Royal Australian Navy's Mine Warfare and Clearance Diving Group recently participated in a demonstration of a programmable micro-influence generator (MIG) used as part of autonomous mine countermeasures. The small device has mine-jamming capabilities and is programmable to simulate magnetic and acoustic signatures able to jam or confuse the firing circuit of a mine. Manufacturer Mission Systems PTY is focusing on increasing the deployability of the device.[47]

[45] David Hambling, "Russia Plans 'Flying Minefield' To Counter Drone Attacks", *Forbes,* 20 April 2021, https://www.forbes.com/sites/davidhambling/2021/04/20/russia-plans-flying-minefield-to-counter-drone-attacks/
[46] Nancy Jones-Bonbrest, "Pentagon completes its first counter-drone technology demonstration", *US Army,* 14 April 2021, , https://www.army.mil/article/245256/pentagon_completes_its_first_counter_drone_technology_demonstration
[47] Lieutenant Commander Alan Parton, "Tech paves way for future anti-mine capabilities", Australian Department of Defense, 30 April 2021, https://news.defence.gov.au/industry/tech-paves-way-future-anti-mine-capabilities

On 26 April, the UK MoD's Defence Science and Technology Laboratory (DSTL) revealed the concept of a Pulse Dart—a metal spike attached to a tube of electronics that can be fired into ordnances such as sea mines. In a video posted on DSTL's website, the inventor of the Pulse Dart, identified only as "Peter", described the motivation for his project, saying "I remember … thinking I wonder what would happen if you electrocuted [a] mine with a couple of hundred thousand volts… I'm guessing it's probably going to explode." Peter also highlighted the cost savings that would come from not using explosives in the counter-mine mission. "It's the handling and storage costs of those explosives that make [mine disposal] prohibitively expensive in some cases."[48]

Robotics and Uncrewed Systems

Key Insights:

- **Lethal Autonomous Weapons Systems and Drone Swarms Have Arrived—Time for a Debate on Norms:** The Turkish Kargu-2 loitering munition was used in combat in Libya to detect, identify, target and strike humans on a battlefield autonomously, according to a UN report released in late May. The incident marked the first known use of a lethal autonomous weapons system against humans and constitutes the crossing of an important threshold that should be of concern for small and large militaries around the world, especially as more countries continue to develop autonomous drone swarm capabilities.
- **UGVs Demonstrate Their Versatility:** The versatility of UGVs were prominently featured in military exercises in Estonia and France in April. In both exercises, variously configured UGVs, including the THeMIS modular UGV developed by Estonian company Milrem, were used to carry out a range of missions—from force protection, to forward reconnaissance, to moving supplies, and even explosive ordnance disposal.
- **The Uncrewed Market Moves Toward Multi-Domain Companies:** While not explicitly covered in this section, the growing demand for uncrewed systems in the air, land, surface, and undersea domains and for the ability to integrate uncrewed systems across these domains is driving mergers and acquisition activities in the uncrewed systems industry. Two separate acquisitions between companies that largely work in separate domains occurred during May. Small uncrewed aerial systems (UAS) manufacturer Aerovironment merged with German uncrewed ground vehicle manufacturer Telerob while uncrewed maritime vehicle company Teledyne acquired FLIR, which makes several small UASs, including the micro-UAS Black Hornet

The Age of Lethal Autonomous Weapons Systems Has Arrived: A United Nations report viewed by *New Scientist* reveals that an uncrewed aerial system (UAS) autonomously identified and attacked human targets in a March 2020 incident in Libya. The incident involved the Turkish made STM Kargu-2 autonomous quadcopter drone—prominently featured in past DEFTECH SCANS for its inclusion of facial recognition software that allowed it to identify and strike individual human targets based on computer vision outputs. According to reporting about the UN document, retreating Haftar Armed Forces were "hunted down and remotely engaged by lethal autonomous weapons systems such as the STM Kargu-2. The systems were programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true 'fire, forget, and find' capability."[49]

[48] "DSTL reaches milestone 1000th intellectual property report", UK.GOV, 26 April 2021, Dstl reaches milestone 1000th intellectual property report - GOV.UK (www.gov.uk)
[49] Daniel Van Boom, "Autonomous drone attacked soldiers in Libya all on its own", *C/Net*, 1 June, 2021, Autonomous drone attacked soldiers in Libya all on its own (msn.com)

The announcement comes amid developing concern about the accelerating pace of development of autonomous drone swarms by more national defence and security communities throughout the world, both large and small. For example, the Bulletin of Atomic Scientists published a paper by national security consultant and US Army "Mad Scientist" Zachary Kallenborn on 5 April 2021 that assessed that "armed, fully-autonomous drone swarms are future weapons of mass destruction." Kallenborn continues by assessing that "while they are unlikely to achieve the scale of harm as the Tsar Bomba, the famous Soviet hydrogen bomb, or most other nuclear weapons, swarms could cause the same level of destruction, death, and injury as the nuclear weapons used in Nagasaki and Hiroshima" due to their ability to combine a capacity for mass destruction and a "lack of control to ensure the weapons do not harm civilians."[50]

Augmented Reality and Drone Swarm Operation

As noted above, militaries are devising and developing more applications for augmented reality, including in supporting drone swarm operations.

In the UK, start-up Blue Bear Systems has developed an augmented reality (AR) system for swarming drones to help enable beyond visual line of sight (BVLOS) operations, according to 21 April reporting from Electronics 360

The technology allows an operator wearing AR glasses to see where the drones in the swarm are and visualize their health status and other parameters. BVLOS capabilities will also enable drone operators to conduct complex drone operations and may possibly be facilitated by the development and deployment of 5G communications that will increase bandwidth, security, and pace of communications.

Source: Peter Brown, "AR system allows operators to see drone swarms", *Electronics 360,* 21 April 2021, AR system allows operators to see drone swarms | Electronics360 (globalspec.com)

At the core of the concern around drone swarms is the potential for "emergent error." Drone swarms rely on the concept of "emergent behavior, the "complex collective behavior that results from the behavior of the individual units" that enables self-healing and other advantageous adaptations. However, the concept loses its efficacy and leads to deleterious outcomes when the algorithms driving intelligent swarms is faulty or incorrect, a possibility that should not be dismissed as "countries rush to develop these weapons."[51]

Ultimately, the paper argues that global norms around drone swarms are urgently needed, particularly around preventing proliferation of intelligent swarms and reenergizing the UN debate on lethal autonomous weapons systems.

[50] Zachary Kallenborn, "Meet the future weapon of mass destruction, the drone swarm", *Bulletin of the Atomic Scientists,* 5 April 2021, Meet the future weapon of mass destruction, the drone swarm - Bulletin of the Atomic Scientists (thebulletin.org)
[51] Ibid.

Demonstrating the Flexibility and Value of Uncrewed Ground Vehicles: In April, the Estonian Defence Forces artillery battalion trialed two Milrem Robotics' THeMIS unmanned ground vehicles (UGVs) during a live-fire exercise.

One UGV was dedicated to combat support and featured an integral FN Herstal defender Light Remote Weapon System (RWS) with a 7.62 mm machine gun. The second UGV operated a tethered drone and provided situational awareness and casualty evacuation. Lieutenant Mari-Li Kapp, commander of the operations and training section of the artillery battalion observed that "having UGVs as a part of the reconnaissance force that prepares the arrival of the main unit, the UGVs could secure the indirect fire and anti-tank teams by providing direct fire support during an engagement and whilst some units are withdrawing. UGVs can also act as front guards all by themselves since they can provide situational awareness and act as forward observers for indirect fire."[52]

Figure 9: The THeMIS in action during the Estonian artillery's live-fire exercise. Source: Milrem via Armada International

Also in April, the French army tested Nexter UGVs, including the armed THeMIS variant Optio-X20. The exercise tested three Nexter systems, all tasked with and configured for different missions: [53]

- The Optio-X20 in missions such as perimeter protection, combat group escort, target acquisition and target engagement
- The Ultra is a cargo carrier UGV
- The Nerva multi-mission reconnaissance and support robot. It can be used for missions such as remote observation, explosive ordnance detection and disposal, and potentially electronic warfare missions, It is reportedly able to be reconfigured within a few seconds in the field with no special tools

[52] Andrew Drwiega, "Estonian Estonian Artillery Deploys UGVs for Fire Support and Situational Awareness - Armada InternationalArtillery Deploys UGVs for Fire Support and Situational Awareness", *Armada International,* 20 May 2021,
[53] "Nexter UGVs tested by French army in defensive and offensive actions", *Army Recognition*, 2 April 2021, Nexter UGVs tested by French army in defensive and offensive actions | Defense News April 2021 Global Security army industry | Defense Security global news industry army year 2021 | Archive News year (armyrecognition.com)


https://deftech.ch/