



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sports DDPS
armasuisse
Science and Technology S+T

DEFTECH SCAN

July 2020



<https://deftech.ch/scans>



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

armasuisse
Inspire
Inform Instruct

Dear Reader,

"May you live in interesting times !"

As indicated by its ironical meaning, we are definitely living in a period far from tranquillity.

Covid-19 might have shaken a little bit our lives, the developments in various technologies are still moving at full speed in all spheres. Substituting the traveling and physical meetings by more reading and digital discussions, we are happy to present you this resilient summer edition of the DEFTECH SCAN.

Before, during (really ?), or after your holidays, we wish you a very nice reading,



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



Dr. Quentin Ladetto
armasuisse S+T
Research director – Technology Foresight
quentin.ladetto@armasuisse.ch

Introduction and Summary

This DEFTECH SCAN reports on and assesses key developments in military technology and capability development taking place in June and July, a reporting period that saw particularly prominent activity in command, control, communication, computers, intelligence, surveillance, and reconnaissance (C4ISR) and unmanned systems capability categories.

As with all DEFTECH SCAN reports, the document includes examples of technology and capability development from defence and security communities across a range of countries with militaries of varying sizes and with different priorities, to include: China, Japan, the United States, United Kingdom, Australia, India, Russia, Canada, Israel, and Germany. Below are key insights emerging from research over the course of this reporting period—including insights from developments not explicitly featured in this report:

World Events Driving Investment in Technology and Capabilities: The combination of intensifying geopolitical competition and the coronavirus pandemic are generating urgency in the development of novel capabilities to meet heightened degree of threat for many nations. For example, Japan’s development of anti-ship hypersonic missiles, establishment of an electronic warfare unit, and domestic development of unmanned underwater vehicle are all part of a focused effort to position the Japanese Self-Defence Force to defend the country’s southwestern islands, especially the Senkakus, which are also claimed by China. Reports during the period that China’s People’s Liberation Army Navy (PLAN) is considering the development of a larger and more capable amphibious assault ship reflects the flipside of the mounting tension over maritime boundary claims across the region, particularly in the South China Sea.

The intersection of geopolitical competition and the global pandemic is also affecting activity in other critical domain areas such as the information domain as evidenced by accusations from the United Kingdom, Canada, and the United States that both Russia and China had launched cyber attacks to steal data related to a coronavirus vaccine during the reporting period.

The Electromagnetic Spectrum: Concern over both friendly and adversary activity (and vulnerability) in the electromagnetic spectrum is also driving innovation of new capabilities, organizational structures, and threats to both small and large military and security communities. Some of these new threats and innovations are reflected in this report—use of jammers by protestors in the United States or growing Department of Defense interest in electromagnetic spectrum visualization and management tools. However, electronic warfare capabilities development during the period goes well-beyond these examples. Consider the release in July by Chinese state-owned media images of an “integrated protection system” that is in service with a brigade of the People’s Liberation Army Rocket Force (PLARF). The system uses jamming rockets to attack incoming missiles, reflecting a continued PLA focus on targeting perceived vulnerabilities of modern militaries—especially the US—in the electromagnetic spectrum.¹

Miniaturization: The integration of emerging technologies into military capabilities is frequently focused on large and exquisite systems and concepts, such as hypersonic missiles, stealth fighters, loyal wingman drones, or even railguns. However, the reporting period saw several examples of militaries focusing on the miniaturization of some of these technologies, including deployment of laser jamming rifles and development of a hand-held electromagnetic railgun. The issue of the threats posed by small weapons and delivery systems was also reflected in intensified concern over the use of small, commercially available (and therefore widely diffused) drones and the asymmetric cost curves associated with meeting these threats.

¹ Samuel Cranny-Evans, “Images emerge of new Chinese vehicle-mounted point protection system”, *Jane’s*, 22 July 2020, <https://www.janes.com/defence-news/news-detail/images-emerge-of-new-chinese-truck-mounted-countermeasures-system>

Energy, Power, and Propulsion

Key Insights:

- An institute associated with the Chinese Academy of Sciences achieved a breakthrough in the viability of scramjet engines constituting a significant development of China's air-launched hypersonic missiles. The achievement also reflects continued progress in China's ability to engineer leading solutions in emerging technology areas likely to shape the future of military capabilities and competition
- Scramjet development may have other applications beyond air-launched hypersonic missiles, including space propulsion.
- Both large and small militaries continue to develop means of increasing the efficiency and power generation of military vehicles including incorporating or refitting existing platforms with hybrid-electric drives that increase performance and lethality.

Chinese Scramjet Breakthrough Establishes a New World Record: A research team at the Chinese Academy of Sciences' Institute of Mechanics claimed a record-setting ground test of a scramjet engine that lasted 600 seconds, according to a statement from the Institute's website. While the precise date of the test was not known, the on-line statement was originally posted in April (and was subsequently removed from the website). The statement became widely reported on in May by various "authoritative local media"² as well as the *South China Morning Post*.³

The previous record of 210 seconds of continuous scramjet engine burn was established by the United States' X-51A Waverider prototype in March 2013. A scramjet accelerated the X-51A to a top speed of Mach 5.1 before its' fuel-load was expended.⁴ In 2016, an Indian test vehicle reached Mach 6, though the engine ran for only five seconds.

Scramjets ("supersonic combustion ramjets") are air-breathing engines that enable aircraft to achieve hypersonic speeds (over Mach 5). The scramjet has no moving parts and uses the forward motion of a plane to compress air and mix it with high-energy fuel to generate explosive thrust. Among the main challenges associated with scramjets has been managing the extreme heat generated by supersonic air streams. The Institute of Mechanics team addressed this problem by "directing fuel to the surface of the most heated components (of the engine), such as the combustion chamber. . . The heat, in turn, would turn the fuel into a gas of carbon and hydrogen molecules eager to meet the oxygen in the compressed air, and burn."⁵

The breakthrough has implications for China's hypersonic weapons program, especially for air-launched hypersonic missiles, and therefore for the intensifying competition in hypersonic missile development. Several countries—including mid-sized militaries such as Japan—are actively developing scramjet engines to support hypersonic missile development. Indeed, in July Japanese Deputy Defense Minister Tomohiro Yamamoto accidentally shared the picture of a model of its under-development hypersonic weapon that is

² Jr Ng, "China advances hypersonic propulsion technologies", *Asian Military Review*, 16 June 2020, <https://asianmilitaryreview.com/2020/06/china-advances-hypersonic-propulsion-technologies/>

³ Stephen Chen, "Report of Chinese scramjet test a challenge to most-advanced missile defence systems", *South China Morning Post*, 31 May 2020, <https://www.scmp.com/news/china/science/article/3086804/report-chinese-scramjet-test-challenge-most-advanced-missile>

⁴ Jr Ng, "China advances hypersonic propulsion technologies", *Asian Military Review*, 16 June 2020, <https://asianmilitaryreview.com/2020/06/china-advances-hypersonic-propulsion-technologies/>

⁵ Stephen Chen, "Report of Chinese scramjet test a challenge to most-advanced missile defence systems", *South China Morning Post*, 31 May 2020, <https://www.scmp.com/news/china/science/article/3086804/report-chinese-scramjet-test-challenge-most-advanced-missile>

based on a “scramjet” (sic) engine on Twitter after visiting the Research Center for Aviation and Rocket Technology outside Tokyo (see Figure 1 below)⁶

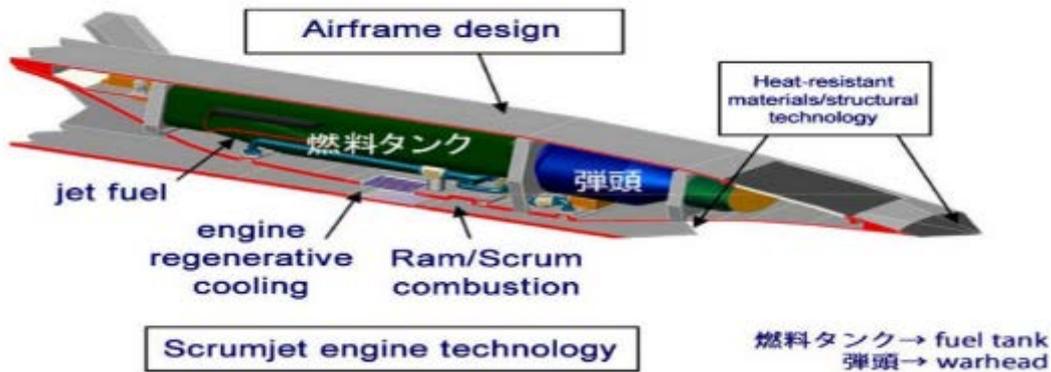


Figure 1:Top” Japanese Deputy Defense Minister Tomohiro Yamamoto visiting the Research Center for Aviation and Rocket Technology, situated close to Tokyo. (Picture source: the Twitter account of Japanese Deputy Defense Minister Tomohiro Yamamoto). Bottom: A diagram of the Acquisition, Technology, and Logistics Agency vision for Japan’s first hypersonic missile, which seeks to use a scram-jet engine that enables hypersonic cruise of a missile using jet fuel, and to develop advanced component technologies for long-time operation of the scram-jet engine. (Picture source: ATLA image)

The team was led by Princeton-educated scientist Fan Xuejun who was nominated by the Chinese Academy of Sciences for a national “innovator of the year” prize, according to the *South China Morning Post*. Fan and his team have also reportedly sought to commercialize the new technology and have established a company in Hefei to produce scramjet engines for future space planes, which could greatly reduce the cost of space flight. The Chinese government has reportedly invested \$28 million in the venture.⁷

Hybrid-Electric Drive Refitting: The US Army’s Rapid Capabilities and Critical Technologies Office (RCCTO) awarded BAE Systems a contract to integrate a Hybrid Electric Drive (HED) onto two A2 Bradley fighting vehicles. BAE Systems will work with QinetQ, which has developed the electric cross drive transmission. The effort is expected to take 24 months and will include “an upgraded engine, a transmission replaced by an electric drive motor, and the addition of lithium ion batteries.”⁸

⁶ Colton Jones, “Japan accidentally leaks image of new hypersonic anti-ship missile”, *Defence Blog*, 9 July 2020, <https://defence-blog.com/news/japan-accidentally-leaks-image-of-new-hypersonic-anti-ship-missile.html>

⁷ Stephen Chen, “Report of Chinese scramjet test a challenge to most-advanced missile defence systems”, *South China Morning Post*, 31 May 2020, <https://www.scmp.com/news/china/science/article/3086804/report-chinese-scramjet-test-challenge-most-advanced-missile>

⁸ “BAE Systems to integrate Hybrid Electric Drive onto a combat vehicle under U.S. Army contract”, BAE Systems press release, 16 July 2020, <https://www.baesystems.com/en-us/article/bae-systems-to-integrate-hybrid-electric-drive-onto-a-combat-vehicle-under>

The HED is expected to “support autonomy, increase power generation, survivability and improve lethality.” According to BAE System’s Ground Vehicles Vice-President Scott Davis, “Integrating a HED system into combat vehicles vastly increases on-board power and provides a significant increase in mobility, lethality options, and range, all of which enable overmatching operational capabilities.”⁹

Human Performance Enhancement and Protection

- Increasing focus on innovation in artificial intelligence (AI) and on human-machine teaming is creating new opportunities for relieving the physical and cognitive burden of human operators, allowing them to focus on higher-value tasks and enhancing their effect in operational environments
- Novel technologies and nearly ubiquitous sensors are also improving human performance by dramatically enhancing situational awareness in contested and cluttered environments and, as a result, allowing for better decision-making and force protection
- Militaries and security communities throughout the world are employing a range of advanced technologies to improve training and force readiness. Technologies such as virtual and augmented reality and cloud computing have been profiled in previous volumes of this report and continue to gain momentum as militaries increasingly turn to synthetic training due both to cost benefits and to circumvent Covid-19 related restrictions.
- However, other novel technologies such as cutting edge non-lethal training ammunition, are also being employed to ensure a high-degree of realism in tactical training

Enhancing Human – Machine Trust: The May 2020 DEFTECH SCAN was dedicated to human-machine interfaces and human – machine interactions. Among the key themes explored in that volume was the growing focus of large and small militaries on building deeper trust between humans and machines in order to facilitate more effective human-machine teaming.¹⁰

In July, the US Defense Advanced Research Projects Agency (DARPA) awarded Calspan Corporation a \$14.1 million, four-year contract to retrofit up to four Aero Vodochody L-39 Albatross jet trainers for artificial controlled flight experiments. The four jets are part of DARPA’s Air Combat Evolution (ACE) program, which is dedicated to improving and measuring human trust in the decision-making abilities of AI agents. The refitted aircraft are part of an effort to develop software capable of carrying out air-to-air combat in order to free up pilots to manage missions and command teams of unmanned vehicles. Part of the refitting contract will be to demonstrate new human-machine interfaces, such as touchscreen displays that will enhance operator efficiency and performance.¹¹

[u-s--army-contract#:~:text=BAE%20Systems%20has%20been%20awarded%20a%20%2432%20million,Drive%20%28HED%29%20system%20onto%20a%20Bradley%20Fighting%20Vehicle.](https://www.baesystems.com/en-us/article/bae-systems-to-integrate-hybrid-electric-drive-onto-a-combat-vehicle-under-u-s-army-contract#:~:text=BAE%20Systems%20has%20been%20awarded%20a%20%2432%20million,Drive%20%28HED%29%20system%20onto%20a%20Bradley%20Fighting%20Vehicle.)

⁹ “BAE Systems to integrate Hybrid Electric Drive onto a combat vehicle under U.S. Army contract”, BAE Systems press release, 16 July 2020, <https://www.baesystems.com/en-us/article/bae-systems-to-integrate-hybrid-electric-drive-onto-a-combat-vehicle-under-u-s-army-contract#:~:text=BAE%20Systems%20has%20been%20awarded%20a%20%2432%20million,Drive%20%28HED%29%20system%20onto%20a%20Bradley%20Fighting%20Vehicle.>

[u-s--army-contract#:~:text=BAE%20Systems%20has%20been%20awarded%20a%20%2432%20million,Drive%20%28HED%29%20system%20onto%20a%20Bradley%20Fighting%20Vehicle.](https://www.baesystems.com/en-us/article/bae-systems-to-integrate-hybrid-electric-drive-onto-a-combat-vehicle-under-u-s-army-contract#:~:text=BAE%20Systems%20has%20been%20awarded%20a%20%2432%20million,Drive%20%28HED%29%20system%20onto%20a%20Bradley%20Fighting%20Vehicle.)

¹⁰ Garrett Reim, “DARPA awards contract to retrofit L-39 Albatross jets for AI dogfighting tests”, *Flight Global*, 9 July 2020

¹¹ Garrett Reim, “DARPA awards contract to retrofit L-39 Albatross jets for AI dogfighting tests”, *Flight Global*, 9 July 2020

More Human-Machine Teaming: During the virtual Future Armoured Vehicle Weapon Systems conference held on 3 – 4 June, Captain Tom Quant Regimental Intelligence Officer and Project Streetfighter Lead at the Royal Tank Regiment of the British Army described a new human-machine teaming concept being tested to protect Challenger 2 tanks and their crews.¹²

The concept involves the use of remote-operated unmanned ground vehicles that would advance ahead of the Challenger 2 tanks. The unmanned vehicles will detect and acquire an enemy and “then send (an) engagement request to tank commander” who would then “consider the tactical situation and approve or deny the fire mission.”¹³

A key component of the concept is Elbit System’s Iron Vision helmet-mounted battlefield situational awareness system. Iron Vision helmet provides the tank commander zero latency 360-degree vision, providing crewmen improved situational awareness in an urban environment. According to Captain Quaint, the system “significantly enhanced awareness, allowing the crew to detect threats and keep track of supporting infantry” during the Fighting In Built Up Areas exercise.¹⁴



Figure 2: A screenshot from the promotional / marketing brochure for Elbit's Iron Vision helmet. The brochure stresses the helmet's ability to provide 360-degree situational awareness and to better operate armored fighting vehicle. Source: Elbit Systems https://elbitsystems.com/media/IronVision_1_Web.pdf

Realistic and Virtual Training: The Australian military demonstrated the importance of emerging technologies for improving the realism of both virtual and live training environments and, as a result, improving readiness of the force to meet the complex challenges of the modern, multi-domain battlefield.

From 26 June to 10 July, the Royal Australian Air Force held the Exercise Virtual Pitch Black. The exercise used a synthetic training environment to deliver complex training scenarios and to connect training audiences from throughout much of the country during a period in which training opportunities have been restricted by Covid-19.¹⁵

Virtual Pitch Black included several mission sets and specialized assets—such as command and control aircraft, fast jets, and intelligence, surveillance, and reconnaissance platforms—and the virtual environment enabled broader participation than live exercises. C-17 pilot Flight Lieutenant Tim Smith commented on the value of virtual exercises for the RAAF: “virtual exercises, through the evolved Air Force synthetic environment, will be able to represent multi-domain contested, degraded and operationally limited environments to satisfy the needs of these next generation capabilities.”¹⁶

¹² “British Armour Trials Unmanned Teaming and Situational Awareness Systems for Urban Canyons”, Asian Military Review, 8 June 2020,

¹³ “British Armour Trials Unmanned Teaming and Situational Awareness Systems for Urban Canyons”, Asian Military Review, 8 June 2020,

¹⁴ “British Armour Trials Unmanned Teaming and Situational Awareness Systems for Urban Canyons”, Asian Military Review, 8 June 2020,

¹⁵ Flight Lieutenant Bel Scott, “Seizing the opportunity for simulated success”, Australian Government, Department of Defence website, 16 July 2020, <https://news.defence.gov.au/capability/seizing-opportunity-simulated-success>

¹⁶ Flight Lieutenant Bel Scott, “Seizing the opportunity for simulated success”, Australian Government, Department of Defence website, 16 July 2020, <https://news.defence.gov.au/capability/seizing-opportunity-simulated-success>

Also during the reporting period, the Royal Australian Army announced that it had begun using “cutting edge” Blue Bolt non-lethal training ammunition (NLTA) in its urban training exercises. The use of NLTA as opposed to blanks in urban training provided a more realistic training environment in which trainees can “fight force-on-force” rather than just against targets and can simulate taking casualties on the battlefield.”¹⁷

Cyber and C4ISTAR

Key Insights:

- Concern about activity and competition in the electromagnetic spectrum is expanding beyond the traditional defense context. This trend has been facilitated by the diffusion of commercially available electronic warfare (EW) attack equipment. EW attacks against the Chicago Police Department during protests in the United States in late May and June reflect a real and disruptive threat for security and law enforcement forces.
- As activity in the electromagnetic spectrum increases so, too, will demand for large and small militaries for systems and organizational structures that will be able not only to detect, visualize, and respond to adversary activity, but also to recognize and deconflict friendly signals.
- Connectivity of military and security personnel in the field and intensified geopolitical competition have created new vulnerabilities related to the use of social media platforms. Intelligence communities are using the access to the social media accounts of military personnel from competitor or adversary nations to gain valuable information about locations of units or equipment or about specific operational procedures and practices. Steps meant to address this threat can create morale challenges and are currently being challenged by military personnel.
- Covid-19 continues to shape conflict in the information domain, both in terms of disinformation campaigns and in the theft of valuable intellectual property related to treatment and vaccine development.

Electronic Warfare and Social Unrest: Large scale protests in the United States related to the death of George Floyd who has asphyxiated by a member of the Minneapolis Police Department on May 25, 2020 have revealed how widely diffused electronic attack techniques and capabilities have become.

According to *Armada International*, reports emerged on 30 May that protestors in Chicago had managed to jam Chicago Police Department (CPD) communications. Frequencies used by police radios were attacked with false voice traffic and music, including Serbian folk music. Local reports indicating the electronic attack activities were “widespread” and not isolated. Dan Casey, the Deputy Director of Public Safety Information at the Office of Emergency Management and Communications (OEMC) for Chicago noted that the jamming could undermine the ability of the police department to deal with a range of challenges throughout the city.¹⁸

The incident also highlights some of the challenges that security and law enforcement communities—especially those in democratic states and societies—have in securing their communication networks in comparison with defence communities and militaries. Radios used by the CPD are not encrypted and use fixed frequency transmission, information about which is available on the internet. Encrypting police communication is not always a viable option in democratic societies as both media and social justice organisations seek to monitor police communications.¹⁹

¹⁷ Major Carrie Robards, “Realistic training gives urban edge”, Australian Government, Department of Defence website, 20 July 2020, <https://news.defence.gov.au/capability/realistic-training-gives-urban-edge>

¹⁸ Dr. Thomas Withington, “Police in a Jam”, *Armada International*, 2 June 2020, <https://armadainternational.com/2020/06/police-in-a-jam/>

¹⁹ Dr. Thomas Withington, “Police in a Jam”, *Armada International*, 2 June 2020, <https://armadainternational.com/2020/06/police-in-a-jam/>

More Electronic Warfare: As the electromagnetic spectrum becomes a more prominent domain of anticipated and on-going conflict, large and small militaries around the world are seeking means of better competing in both electronic attack and defence.

In July, the Japan Ground Self-Defence Force (JGSDF) announced it will establish a new EW unit at Camp Kengun on Kyushu Island in the spring of 2021. The unit is expected to consist of approximately 80 personnel and will be tasked to detect and identify enemy naval and airborne communication and radar emissions and then use this information to jam the enemy's radar and missile seekers. The unit will also protect the JGSDF's own communications links.²⁰

The unit is expected to coordinate closely with the Amphibious Rapid Deployment Brigade (ARDB), which was launched in March 2018 and is also based on Kyushu Island. The ARDB, along with the development of hypersonic weapons, are also part of Japan's effort to defend its southwestern islands, particularly the Senkaku Islands, which are also claimed by China.²¹

The US Army also announced that its Electronic Warfare Planning and Management Tool (EWPMT) is being considered as an option for the joint force to coordinate actions across the electromagnetic spectrum.

“We’re going to continue to have more sensors that are on the battlefield that we need to continue to be able to do the planning and management of and simulation of and then also be able to integrate with our joint forces.” – Colonel Kevin Finch

The system is designed to help commanders and operators to visualize adversary activity in the EM spectrum. Some countries, such as Russia, have displayed the capability to “[geolocate] units based solely on their electromagnetic footprint, revealing their location, and then targeting those units with munitions.”²²

It is also designed to plan, deconflict, and manage friendly signals. Colonel Kevin Finch, a Program Manager for Electronic Warfare and Cyber within Program Executive Office Intelligence, Electronic Warfare and Sensors outlined the nature of the challenge EWPMT is meant to address: “We’re going to continue to have more sensors that are on the battlefield that we need to continue to be able to do the planning and management of and simulation of and then also be able to integrate with our joint forces.”²³

Raytheon is developing the EWPMT via a series of “capability drops” or incremental software instalments. Current work is on drop 4, which will allow for increased visualization of the environment of potential effects up to division and corps level. The EWPMT capability is also being integrated into the Army's Command Post Computing Environment, which consolidates disparate command post tools into a single user interface within the brigade tactical operations centre.

²⁰ Kosuke Takahashi, “JGSDF to form new EW unit to defend Japan's southern remote islands”, *Jane's*, 2 July 2020, <https://www.janes.com/defence-news/jgsdf-to-form-new-ew-unit-to-defend-japans-southern-remote-islands/>

²¹ Tate Nurkin and Ryo Hinata-Yamaguchi, “Emerging technologies and the future of US-Japan defense collaboration”, Atlantic Council, 17 April 2020, <https://www.atlanticcouncil.org/in-depth-research-reports/report/emerging-defense-technologies-and-the-future-of-us-japan-defense-collaboration/>

²² Mark Pomerleau, “The Army may have the electronic warfare tool the Pentagon needs”, *C4ISRNET*, 15 June 2020, <https://www.c4isrnet.com/electronic-warfare/2020/06/15/the-army-may-have-the-electronic-warfare-tool-the-pentagon-needs/>

²³ Mark Pomerleau, “The Army may have the electronic warfare tool the Pentagon needs”, *C4ISRNET*, 15 June 2020, <https://www.c4isrnet.com/electronic-warfare/2020/06/15/the-army-may-have-the-electronic-warfare-tool-the-pentagon-needs/>

Indian Army Bans 89 Apps: The Indian Army mandated that personnel delete 89 apps from their mobile phones due to operational security concerns, including Facebook, Instagram, and 59 with Chinese links. The Indian Army had previously banned use of WhatsApp for official work in November 2019.²⁴

Concerns over social media activity are layered. There have been cases in the last several years in which Pakistani agents posing as women have convinced military personnel into divulging classified information. Some military personnel have been court-martialled for posting sensitive or classified information—for example, the location of a unit—on social networking websites.²⁵ In addition, the prevalence of Chinese-developed or owned apps also reflects a broader information / cyber security concern, especially in light of the recent conflict between China and India.

A protest against the order was filed by Lt. Colonel PK Choudhary soon after its release on 6 June. Lt. Colonel Choudhary—who is stationed in Jammu and Kashmir—claimed the order was a violation of his fundamental rights and that he needed to be able to access Facebook to communicate with friends and relatives throughout the world. The protest was originally rejected, and Lt. Colonel Choudhary was told to delete relevant apps or resign from the Army.

That decision was reversed, and the protest was heard on a video teleconference on 21 July²⁶, reflecting the difficulty for small and large militaries in maintaining balance between operational security and soldier morale in an environment marked by both connectivity and competition. A heightened degree of social media use is expanding the connective of soldiers in the friends to their friends, family, and the outside world while accelerating geopolitical competition is driving near constant sub-threshold efforts to exploit this salutary connectivity for tactical, operational, or strategic advantage.

Covid-19 and Cyber Conflict: The governments of the United States, United Kingdom, and Canada accused Russian state intelligence of hacking international research centres involved in the development of Covid-19 vaccines on 16 July.

Britain’s National Cyber Security Centre (NCSC) released a statement indicating that vaccine and therapeutic sectors in multiple countries have been targeted by a group known as APT29 (also known as “Cozy Bear”) which is “almost certainly” part of Russian state intelligence. The NCSC statement was echoed by statements from the United States and Canadian intelligence communities. Two notable victims of Cozy Bear’s hacking efforts were Oxford University and AstraZeneca, a British -Swedish pharmaceutical company, both of which are “leading candidates to develop a viable coronavirus vaccine” that have recently announced progress toward this objective.²⁷

The US National Security Agency (NSA) noted that US-based organisations involved in vaccine development were targeted by hackers with the intent “to steal information and intellectual property relating to the development and testing of Covid-19 vaccines.” The Canadian government announced it is working closely with the British government to address “malicious cyber activities” as well.²⁸

²⁴ “Army asks soldiers, officers to delete Dailyhunt, Facebook and Instagram; uninstall 89 apps”, *The Times of India*, 8 July 2020, <https://timesofindia.indiatimes.com/india/army-asks-soldiers-officers-to-delete-dailyhunt-facebook-and-instagram-uninstall-89-apps/articleshow/76858779.cms>

²⁵ “Army asks soldiers, officers to delete Dailyhunt, Facebook and Instagram; uninstall 89 apps”, *The Times of India*, 8 July 2020, <https://timesofindia.indiatimes.com/india/army-asks-soldiers-officers-to-delete-dailyhunt-facebook-and-instagram-uninstall-89-apps/articleshow/76858779.cms>

²⁶ “Army officer challenges Indian Army’s social media ban; Delhi High Court orders in-camera proceedings”, *Orissa Post*, 21 July 2020, <https://www.orissapost.com/army-officer-challenges-indian-armys-social-media-ban-delhi-high-court-orders-in-camera-proceedings/>

²⁷ “Vaccine Hacking: The Latest Trend in Cyberwarfare and Digital Espionage”, *The Soufan Center*, 24 July 2020, <https://thesoufancenter.org/intelbrief-vaccine-hacking-the-latest-trend-in-cyberwarfare-and-digital-espionage/>

²⁸ Kitty Donaldson, Ryan Gallagher, and Chris Strohm, “Russian Hackers Are Linked to Sweeping Bid to Steal Vaccine Data”, *Bloomberg*, 16 July 2020, <https://www.bloombergquint.com/coronavirus-outbreak/u-k-says-russians-are-trying-to-steal-covid-19-vaccine-research>

The US government has also accused China of hacking US-based organizations in order to gain vaccine-related information, among other sensitive intellectual property. The US Department of Justice indicted two purported Chinese engineering students – Li Xiaoyu and Dong Jiazifor—for hacking companies engaged in high-tech manufacturing, pharmaceuticals and gaming software development. Significantly, the indictment states that the two individuals hacked for their own personal profit but also on behalf of China’s Ministry of State Security (MSS). The indictment also accuses the two individuals and the Chinese government with targeting dissidents, clergy and human rights activists in the United States, China and Hong Kong.²⁹

Manned Platforms

Key Insights:

- Russia continues to develop and display advanced military capabilities, especially in land systems. The Armata family of tanks and land vehicles was prominently featured in the delayed Victory Day parade held in Moscow on 24 June. Many of the tanks and fighting vehicles displayed in Moscow are also being made available for export and will also be featured at the upcoming Army 2020 defence exhibition being held in Mosco in August. As a result, Russia’s continued focus on manned land vehicles is likely to be of interest to and concern for a broad array of military and security communities throughout the world.
- Global events continue to shape the prioritization of capabilities that militaries of all sizes are pursuing. The release of information during the reporting period about a new more capable People’s Liberation Army Navy (PLAN) amphibious assault ship is likely a response to the growing tensions between China and its many regional neighbors as well as the United States over China’s increasingly aggressive territorial claims in the East and South China Seas.
- The incorporation of an electromagnetic launch catapult in the design of the new amphibious assault craft reflects a growing interest in a critical advanced technology even as a United States’ Ford class aircraft carrier experienced a significant technical challenge with its electromagnetic catapult that inhibited the aircraft carrier from launching planes for five days during testing.

Russian Armour on Display: Russia demonstrated a range of new and modernized military equipment during its Victory Day parade commemorating Germany’s surrender in World War II on 24 June. The parade was originally scheduled for 9 May but was delayed due to coronavirus concerns.

According to *Jane’s*, equipment featured in the parade was mainly newly designed land systems, including six T-90M Proryv tanks, seven T-80BVMs, and seven T-72B3M obr.2016 systems, which had not been previously displayed in Victory Day parades. The Proryvs included flexible nets with heavy protection of the lower part of the turret against high-explosive anti-tank munitions.³⁰

The Victory Parade line-up also consisted of several members of the Armata family of heavy armoured vehicles, such as four T-14 main battle tanks and three updated T-15 Armata heavy infantry fighting vehicles (IFV). The IFV had a “modernized Kinzhal remotely operated weapon station with a 57 mm main gun, a Kalashnikov PKTM 7.62 mm general-purpose machine gun, and two anti-tank guided missiles in a protected two-cell bank mounted on the right of the vehicle.”³¹

²⁹ Ellen Nakashima and Devlin Barrett, “U.S. accuses China of sponsoring criminal hackers targeting coronavirus vaccine research”, *Washington Post*, 21 July 2020, https://www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html

³⁰ Dmitry Fediushko and Nikolai Novichkov, “Delayed Victory Day parade features new and upgraded Russian land systems”, *Jane’s*, 24 June 2020, <https://www.janes.com/defence-news/news-detail/delayed-victory-day-parade-features-new-and-upgraded-russian-land-systems>

³¹ Dmitry Fediushko and Nikolai Novichkov, “Delayed Victory Day parade features new and upgraded Russian land systems”, *Jane’s*, 24 June 2020, <https://www.janes.com/defence-news/news-detail/delayed-victory-day-parade-features-new-and-upgraded-russian-land-systems>

The T-14 MBT and T-15 tank support fighting vehicle are also among the manned platforms expected to be displayed at the Army – 2020 defence exhibition scheduled to be held in Moscow from 23 -29 August, Alexander Mikheyev, the CEO of Russia’s state arms exporter, Rosoboronexport announced in June. Army-2020 is “the first major event for the global defence industry following the lifting of restrictions caused by the Covid-19 pandemic” and offers Russia an opportunity to advance or secure deals for its new and modernized equipment as well as broader military-technical cooperation with foreign countries.

The Ups and Downs of Electromagnetic Launch: Chinese shipbuilder China Shipbuilder Group has released plans to build a more powerful amphibious assault ship that not only would be able to carry more helicopters and unmanned systems, but also would utilize an electromagnetic catapult launch system.



Figure 3: An image of the proposed design of the Type 076 amphibious assault ship that has been circulating on Chinese military websites. Source: South China Morning Post, <https://www.scmp.com/print/news/china/military/article/3094912/chinese-shipbuilder-planning-advanced-amphibious-assault-ship>

The new design – informally known as the Type 076—would be similar in size to the Type 075, which was launched earlier this year, but is not yet in service. The Type 076 is expected to be larger and will be able to carry up to 30 helicopters as well as amphibious tanks, armoured vehicles, boats, and hundreds of marine troops for amphibious assaults. Naval commentator, Li Jie, noted that the ship would be well suited to a combat role focused “on the high seas when China is facing territorial challenges from rival claimants in the region.”³² China has several active maritime territorial disputes, including as noted above with Japan over the Senkaku Islands, and with several other claimants in the South China Sea. Tensions in the South China Sea have intensified over the spring and summer of this year as China has attempted to press its claims while several other claimants, notably Vietnam and Malaysia, and other states, such as the United States, Indonesia, and Australia, have more assertively pushed back on these claims.

The inclusion of an electromagnetic catapult launch system is particularly noteworthy and is perhaps the most significant technical challenge to the future development of the Type 076, given that China has yet to successfully integrate this technology on its full-sized aircraft carriers. The People’s Liberation Army Navy’s (PLAN) second aircraft carrier, the *Shandong*, entered service in December 2019 and utilizes a “ski ramp” launch. The currently under-development Type 002 aircraft carrier is expected to be fitted with the electromagnetic catapult. As Li noted “only when the new Type 002 aircraft carrier finishes testing the three electromagnetic catapult can we make sure it’s a mature technology that could be applied on the flight deck of the Type 075.”³³

Notably, the challenges associated with electromagnetic catapult launch were highlighted during the reporting period. In early June, the crew of the USS *Gerald R. Ford* (CVN-78) Ford-class aircraft carrier identified a fault

³² Minnie Chan, “Chinese shipbuilder planning advanced amphibious assault ship”, *South China Morning Post*, 27 July 2020, <https://www.scmp.com/news/china/military/article/3094912/chinese-shipbuilder-planning-advanced-amphibious-assault-ship>

³³ Minnie Chan, “Chinese shipbuilder planning advanced amphibious assault ship”, *South China Morning Post*, 27 July 2020, <https://www.scmp.com/news/china/military/article/3094912/chinese-shipbuilder-planning-advanced-amphibious-assault-ship>

in the power handling system that connects the ship's energy – generating turbines to the ship's Electromagnetic Aircraft Launch System (EMALS). The result was that the *Gerald R. Ford* was unable to launch aircraft for five days during its latest at-sea testing period.³⁴ The US Navy was quick to highlight that the challenge with the EMALS system was an isolated issue not a systemic problem that will undermine further use of EMALS. James Guerts, the Assistant US Navy Secretary for Research, Development, and Acquisition assessed that “Nothing we have seen, nothing I know of and nothing we’re talking about is a landmine or an Achilles Heel in the system.”³⁵ The Navy also released a statement reiterating that “to date, *Ford* has conducted 3,480 catapult launches and arrested landings with EMALS and [Advanced Arresting Gear].”³⁶

Missile Systems and Munitions

Key Insights:

- The miniaturization of key technologies and capabilities is creating new opportunities for the deployment of novel weapons, such as hand-held laser and railgun weapons as well as small missile interceptors designed to enhance platform and personnel survivability
- Space continues to be a highly competitive domain as Russia reportedly tested an on-orbit, space-based counter-space capability. Russia's test is another in a growing list of demonstrations of a set of counter-space / anti-satellite capabilities, ranging from direct ascent anti-satellite weapons to ground (or, plausibly, space)-based directed energy, to cyber attacks to co-orbital or kamikaze satellites.

³⁴ Sam Lagrone, “USS Gerald Ford EMALS Launching System Suffers Fault During Testing Period”, *USNI News*, 8 June 2020, <https://news.usni.org/2020/06/08/uss-gerald-ford-emals-launching-system-suffers-fault-during-testing-period>

³⁵ Michael Fabey, “EMALS problems do not represent ‘Achilles Heel’ for launch system, US Navy assistant secretary says”, *Jane's*, 19 June 2020, <https://www.janes.com/defence-news/news-detail/emals-problems-do-not-represent-achilles-heel-for-launch-system-us-navy-assistant-secretary-says>

³⁶ Sam Lagrone, “USS Gerald Ford EMALS Launching System Suffers Fault During Testing Period”, *USNI News*, 8 June 2020, <https://news.usni.org/2020/06/08/uss-gerald-ford-emals-launching-system-suffers-fault-during-testing-period>

Star Wars Weapons (Part 1): Hand-Held Laser Weapons: The US Navy released a photo in July of the Virginia-class nuclear submarine *USS Minnesota* that showed a sailor carrying a hand-held laser-dazzler weapon known as the B.E. Meyers Glare LA-9/P.³⁷

The weapon fires powerful and precise laser beams over long distances that blinds attackers (or the electro-optic systems on an attacking platform). The US Navy uses the weapon as a means of platform protection when submarines have surfaced and are more vulnerable to fast-attack boats, armed unmanned systems, or loitering munitions.

The Glare LA-9/P is just one laser dazzler in use by the US Navy. According to *The Drive*, a more powerful and hard – mounted laser dazzler with extended range named ODIN is already deployed on a Navy destroyer and is planned to be deployed on seven more over the next three years.³⁸

Also during the reporting period, China’s People’s Liberation Army (PLA) demonstrated a miniaturized electromagnetic railgun and pistol-and rifle-sized synchronous induction coilgun prototypes. The weapons were developed by the PLA Army Logistics University.

The coilgun fires bullets stored in a reloadable magazine—similar to a conventional weapon—but accelerate bullets through the barrel using electromagnetic force, meaning that the projectile is fired at a much higher rate. According to multiple reports on the demonstration, projectiles fired by miniaturized electromagnetic coilguns “can easily penetrate multiple wood plates and thin steel plates at relatively close distance.”³⁹

The weapon is still at the prototype stage. Improvements in “battery or capacitor capacity to store and release energy” are still required to improve range.⁴⁰

Star Wars Weapons (Part 2): Space-Based Anti-Satellite Weapons: On 23 July, the United States and United Kingdom accused Russia of testing a weapon-like projectile launched from a satellite in orbit that could be used to target other satellites in orbit.



Figure 4: Top Image: A US sailor armed with a handheld laser dazzler weapon on top of the surfaced *USS Minnesota*, <https://www.thedrive.com/the-war-zone/35106/check-out-this-sailor-holding-a-laser-dazzler-rifle-aboard-nuclear-submarine-uss-minnesota> Bottom Image: A released image of a Chinese soldier firing the handheld electromagnetic railgun. <http://www.globaltimes.cn/content/1192841.shtml>

³⁷ Tyler Rogoway, “Check Out This Sailor Holding A Laser Rifle Aboard the Nuclear Submarine *USS Minnesota*”, *The Drive*, 26 July 2020, <https://www.thedrive.com/the-war-zone/35106/check-out-this-sailor-holding-a-laser-dazzler-rifle-aboard-nuclear-submarine-uss-minnesota>

³⁸ Tyler Rogoway, “Check Out This Sailor Holding A Laser Rifle Aboard the Nuclear Submarine *USS Minnesota*”, *The Drive*, 26 July 2020, <https://www.thedrive.com/the-war-zone/35106/check-out-this-sailor-holding-a-laser-dazzler-rifle-aboard-nuclear-submarine-uss-minnesota>

³⁹ Liu Xuanzun, “Chinese military reveals rifle-sized railgun prototypes”, *The Global Times*, 28 June 2020, <http://www.globaltimes.cn/content/1192841.shtml>

⁴⁰ Liu Xuanzun, “Chinese military reveals rifle-sized railgun prototypes”, *The Global Times*, 28 June 2020, <http://www.globaltimes.cn/content/1192841.shtml>

According to a US Space Command (USSC) 15 July statement, Russia “injected a new object into orbit” from the Cosmos 2543 satellite and “conducted a non-destructive test of a space-based anti-satellite weapon.”⁴¹ During the test, Russia released the new object near to another Russian satellite, purportedly to inspect the second satellite, though the US Department of State described the projectile’s activity as “inconsistent with their stated mission.”⁴² According to both the US Department of State and the head of the UK’s space directorate, Air Vice Marshal Harvey Smyth, the projectile had “characteristics of a weapon.”⁴³

Concern over “co-orbital” satellites that can damage satellites in orbit using a robotic arm or potentially a directed energy weapon and “kamikaze” satellites that are launched against satellites in space is not new. Indeed, the US government has frequently expressed concern over the increasing sophistication of China’s range of counterspace capabilities that go well-beyond the blunt instrument of direct ascent anti-satellite missiles.⁴⁴ Clearly, the recent Russian test has brought the issue of competition, escalation, and conflict in space back into prominence, especially in conjunction with an incident in February in which two Russian satellites maneuvered close to an American one and an April test of a Russian ground-based anti-satellite weapon.

“Tiny” Missile Interceptor for Survivability: On 21 July, the US Department of Defense announced that Raytheon had been awarded a \$375 million contract to provide a small interceptor to defend aircraft against enemy missile attacks. The first phase of the award was for \$93 million with an expectation that the missile will be flight test ready by October 2023.

The award is part of the Air Force Research Lab’s (AFRL) Miniature Self-Defense Munition (MSDM) program, which first emerged in 2015. Little has been revealed about the program over the past five years, though AFRL has previously stated that the weapon should be “extremely-agile, highly-responsive” and have “minimal impact to platform payload capacity.”⁴⁵ The desired length for the “miniature” missile will be around one meter, making the missile about a third as long as the AIM-9X Sidewinder air-to-air missile.⁴⁶

A key component of the missile will also be its “very low cost passive seeker, thought to be a imaging infrared seeker, which “would give the missile of means of finding its target that is immune to electronic warfare jamming.” The missile is expected to be just one layer of defence for a wide range of manned (and eventually unmanned) aircraft, including fighter jets, bombers, intelligence platforms, aerial refuelers and transport aircraft.

⁴¹ Chelsea Gohd, “Russia has tested an anti-satellite weapon in space, US Space Command says”, *Space.com*, 23 July 2020, <https://www.space.com/russia-tests-anti-satellite-weapon-in-space.html>

⁴² Chelsea Gohd, “Russia has tested an anti-satellite weapon in space, US Space Command says”, *Space.com*, 23 July 2020, <https://www.space.com/russia-tests-anti-satellite-weapon-in-space.html>

⁴³ “UK and US say Russia fired a satellite weapon in space”, *BBC.com*, 23 July 2020, <https://www.bbc.com/news/world-europe-53518238>

⁴⁴ Tate Nurkin et al., “China’s Advanced Weapons Systems”, *Jane’s by IHS Markit* prepared for the US-China Economic and Security Review Commission, May 2018, https://www.uscc.gov/sites/default/files/Research/Jane%27s%20by%20IHS%20Markit_China%27s%20Advanced%20Weapons%20Systems.pdf

⁴⁵ Joseph Trevithick, “Tiny Missile Interceptor To Defend Aircraft Against Enemy Missile Attacks Moves Forward”, *The Drive*, 22 July 2020, <https://www.thedrive.com/the-war-zone/35038/tiny-missile-interceptor-to-defend-aircraft-against-enemy-missile-attacks-moves-forward>

⁴⁶ Joseph Trevithick, “Tiny Missile Interceptor To Defend Aircraft Against Enemy Missile Attacks Moves Forward”, *The Drive*, 22 July 2020, <https://www.thedrive.com/the-war-zone/35038/tiny-missile-interceptor-to-defend-aircraft-against-enemy-missile-attacks-moves-forward>

Robotics and Unmanned Systems

Key Insights:

- Development by large, mid-sized, and small militaries of unmanned systems designed to operate in difficult environments has continued. Of particular note during the period was Japan's continued development of unmanned underwater vehicles to better compete in the undersea domain and Russia's development of unmanned rotorcraft to be able to operate more freely in the Arctic.
- The diffusion of small, low cost, commercially available drones is beginning to overwhelm the capacity of defence and security communities of varying sizes and degrees of sophistication to effectively defend against these risks to military assets, personnel, and facilities as well as critical infrastructure.
- The proliferation of these drones was creating demand for novel counter-drone approaches, including the use of interceptor drones.

Dull, Dirty, and Dangerous Missions: Among the many layers of value unmanned systems provide is their capacity to more efficiently and safely operate in dull, dirty, and dangerous environments that challenge human physical and cognitive limits.

Over the course of the reporting period, militaries throughout the world developed solutions for operating in specific dull, dirty, and / or dangerous environments that have already become or are likely to become the focus of increased military and geopolitical competition, namely the undersea domain and the Arctic.

On June 23, Japan's Ministry of Defence (MoD) told *Jane's* that it seeks to develop two prototypes of a remotely operated, self-propelled mine system, which the MoD described as "small expendable wireless unmanned underwater vehicles." The systems are designed to be deployed to high-risk sea areas and loiter there until they are remotely detonated in the proximity of enemy vessels. The prototypes are part of a broader Japanese effort to indigenously design and develop UUV (Unmanned Underwater Vehicle) technologies, including a contract with Mitsubishi Heavy Industries, for "exchangeable modules and mission payloads."⁴⁷

⁴⁷ Kosuke Takahashi, "Japan aiming to develop prototypes of self-propelled mine system", *Jane's*, 23 June 2020, <https://www.janes.com/defence-news/news-detail/japan-aiming-to-develop-prototypes-of-self-propelled-mine-system>



Figure 5: The ERA-100. Source: Rostec and Aeroxo Group, <http://aeroxogroup.com/tech.html>

Also in June, Russian defence firm Rostec announced it is partnering with start-up Aeroxo to make tiltrotor drones to operate in the Arctic. Rostec and Aeroxo will build Aeroxo’s existing ERA-100, a four-engine tiltrotor with a six-foot wingspan, a 5.5-pound lifting capacity and a range of around 75 miles at a top speed of 75 miles per hour.⁴⁸

Operating in the Arctic is particularly difficult, not only because of the extreme cold, but also due to “mountain ranges, icing conditions, volatile sea states, unpredictable sea ice . . . and large swings in seasonal daylight, all with a lack of support or communications infrastructure.”⁴⁹

The co-development of the tilt-rotor aircraft will be critical to Russia’s growing Arctic ambitions and operations. Samuel Bendett, an Advisor at the Center for Naval Analysis explains that “Russia will be investing in its Arctic infrastructure both to tap the natural resources and to secure the Northern Route for the impending rise of sea-based traffic.”

Diffusion of Small Drones is Overwhelming Defence and Security Communities: The diffusion of small, commercially available drones is posing a tactical, operational, and—increasingly—strategic challenge for small and large militaries, including the most well-equipped military in the world.

In a virtual event hosted by the Middle East Institute in Washington, DC, General Kenneth McKenzie, the commanding officer of the US Central Command (CENTCOM) stressed the growing asymmetries associated with defending against attacks from militant groups operating in the region. General McKenzie’s assessment was that “right now, the fact of the matter is [the United States military in the Middle East] is on the wrong side of the equation. We’re working very hard to fix it. It concerns me.”⁵⁰

Of central concern is the availability of small, hard-to-detect systems flying at low velocity and altitude that can be easily modified to create threats to personnel, equipment, and facilities. According to General McKensie, “I’m not talking about large unmanned platforms, which are the size of a conventional fighter jet that we can see and deal with. I’m talking about the one you can go out and buy at Costco right now in the United States for a thousand dollars, four quad, rotorcraft or something like that that can be launched and flown.”⁵¹

⁴⁸ David Axe, “The Arctic Eats Helicopters, So Russia Is Sending Drones Instead”, *Forbes*, 21 June 2020, <https://www.forbes.com/sites/davidaxe/2020/06/21/the-arctic-eats-helicopters-so-russia-is-sending-drones-instead/#52c3ffd5103e>

⁴⁹ David Axe, “The Arctic Eats Helicopters, So Russia Is Sending Drones Instead”, *Forbes*, 21 June 2020, <https://www.forbes.com/sites/davidaxe/2020/06/21/the-arctic-eats-helicopters-so-russia-is-sending-drones-instead/#52c3ffd5103e>

⁵⁰ Jared Keller, “CENTCOM chief: US troops can’t keep up with the flood of cheap drones downrange”, *Task and Purpose*, 12 June 2020, <https://taskandpurpose.com/news/drone-swarms-middle-east-centcom>

⁵¹ Jared Keller, “CENTCOM chief: US troops can’t keep up with the flood of cheap drones downrange”, *Task and Purpose*, 12 June 2020, <https://taskandpurpose.com/news/drone-swarms-middle-east-centcom>

Of course, the United States is not the only country operating in the Middle East or elsewhere expressing concern about the prevalence of small commercially available drones being modified to drop bombs or grenades on military assets or even critical infrastructure. A December 2019 article in the *Bundeswehr Journal* noted that “cheap drones are currently experiencing a real boom. However, their reconnaissance and payload capability, such as explosive devices can also make them a threat to military and civilian facilities.



Figure 6: An image of the Drone Guard counter-drone system, Source: Israeli Aerospace Industries via Jane’s, <https://www.janes.com/defence-news/news-detail/iai-drone-guard-gets-guard-drones>

Terrorists and criminals, as well as thoughtless hobbyists, can do enormous damage with drones.”⁵²

A May 2020 Atlantic Council report entitled “Drone Attacks Against Critical Infrastructure: A Real and Present Threat” underscores the scale of the challenge, noting that since July 2018, “there have been more than one hundred attacks by unmanned aerial systems against commercial airports and military air bases in the Middle East and North Africa.”⁵³

The result of this proliferation and use of modified small drone attacks against military personnel and critical infrastructure is catalysing even more demand for counter-drone weapons. Indeed, during the reporting period and in response to the growing small drone threat, Israeli Aerospace Industries (IAI) announced that it has integrated

interceptor drones as part of its Drone Guard counter-UAV system after signing a contract with Iron Drone, which manufactures the Iron Drone interceptor.⁵⁴

Other Unmanned Developments of Interest: The reporting period had a particularly high degree of activity related to military, security, and even commercial drone development. Below are a series of *representative examples* of activity of interest that reflect broader relevant trends from this report and in the unmanned systems market, and prioritized capabilities.

- **Milrem Robotics** announced the development of the Type-X Robotic Combat Vehicle (RCV), which is supposed to “replace conventional fighting vehicles that are used to transport soldiers.” The vehicle, much like the Japanese and Russian systems discussed above, is intended to reduce the number of soldiers deployed to dangerous environments while preserving the same fighting power.⁵⁵
- **FLIR** was awarded a contract with the US Army to continue to supply the Black Hornet 3, a nano-sized Personal Reconnaissance System UAV. The drone’s sensors allow it to transmit live video and high-definition images back to an operator across a secure data link, similar to the concept explored for ensuring the safety of Challenge 2 tanks and their crews in the Human Performance Enhancement and Protection section of this paper. Black Hornet 3s weigh only 33 grams and are easily transported by individual troops.⁵⁶
- **Patria** reached a new milestone in the development of its Heavy Unmanned Ground Vehicles program. On 7 June, the company released a statement that the Patria AMV 8x8 vehicle can now be

⁵² “Drone defense with Protector RWS from Kongsberg”, *Bundeswehr Journal*, 6 December 2019, <http://www.bundeswehr-journal.de/2019/drohnenabwehr-mit-protector-rws-von-kongsberg/>

⁵³ Dr. Scott Crino and Conrad “Andy” Derby, “Drone Attacks Against Critical Infrastructure”, Atlantic Council, May 2020, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/drone-attacks-against-critical-infrastructure-a-real-and-present-threat/>

⁵⁴ Yaakov Lappin, “IAI Drone Guard gets guard drones”, *Jane’s*, 1 July 2020, <https://www.janes.com/defence-news/news-detail/iai-drone-guard-gets-guard-drones>

⁵⁵ “Milrem Robotics’ Swedish and Estonian engineers developing the world’s most modern fighting vehicle”, Milrem Robotics website, 16 June 2020, <https://milremrobotics.com/milrem-robotics-swedish-and-estonian-engineers-developing-the-worlds-most-modern-fighting-vehicle/>

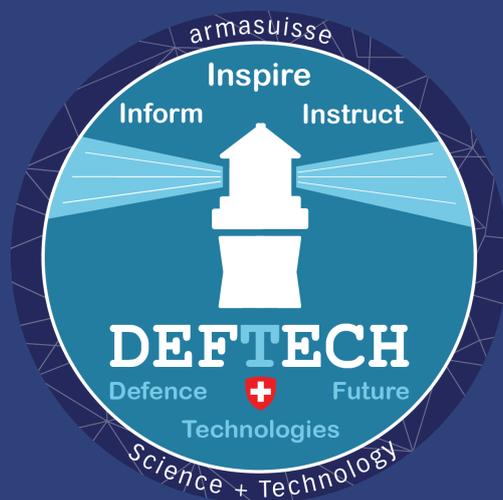
⁵⁶ Dave Makicuk, “FLIR’s Black Hornet 3 nano drone seeks to destroy”, *Asia Times*, 18 June 2020, <https://asiatimes.com/2020/06/flir-nets-contract-for-black-hornet-3-nano-drones/>

operated remotely beyond visual line of sight utilizing 5G and 4G networks. The demonstration of this new capability also incorporated other emerging technologies—stressing the amplifying intersections of these technologies for defense. Notably, the demonstration included new interfaces such as augmented reality and haptic feedbacks to ensure efficiency and performance of remote operators.⁵⁷

- **Boston Dynamics** placed its four-legged robot Spot on general sale and as of mid-July is allowing any US firm to buy a copy for \$74,500. The robot is currently optimized for surveying and data collection and placing sensors where companies do not want people to go. While Spot is mainly meant to be operated remotely, the upgraded version being offered has enhanced autonomy and navigation. The company has established a code of use for Spot that prohibits weapon attachments or any use case that involves harming or intimidating people. Still, the diffusion of these commercial systems open up new opportunities for creative and malign uses that could pose challenges to both small and large defence and security communities.⁵⁸

⁵⁷ “Patria reached a new milestone in the capabilities of Heavy Unmanned Ground Vehicles”, Patria Group news release, 6 July 2020, <https://www.patriagroup.com/newsroom/news/2020/patria-reached-a-new-milestone-in-the-capabilities-of-heavy-unmanned-ground-vehicles>

⁵⁸ James Vincent, “Boston Dynamics will now sell any business its own Spot robot for \$74,500”, *The Verge*, 16 June 2020, <https://www.theverge.com/21292684/boston-dynamics-spot-robot-on-sale-price>



<https://deftech.ch>