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

November 2019

https://deftech.ch/scans

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

Dear Reader,

Time flies and we are proud to present you here the last edition of the DEFTECH "scan" for year 2019. Do not worry; we will be back in January!

You will find in this release some new designs of products that were presented in different part of the world during various commercial or national event. At this stage, it is not always obvious to differentiate between national propaganda and real new capabilities, but efforts to ensure deterrence and military superiority are there. You will find all these insights summarized following our well-known structure:

- Energy and Power
- Human Performance Enhancement
- Cyber and C4ISTAR
- Manned Platforms
- Missile Systems and Munitions
- Robotics and Unmanned Systems

We have added some "key insights" parts that help a quick reading, but we hope you will be interested by the details as well. Do not hesitate to visit the various links to continue the journey.

In 2020, some of the "burning" themes will be the topics of the DEFTECH-DAYS to which you are welcome to participate.

- May 5th 2020: Human-Machin Interface & Interaction
- September 17th 2020: High Altitude Platforms (HAPS)
- November 10th 2020: Hypervelocity Missiles

More information and programs will be available here: https://deftech.ch/d-days

We do hope you will find this 2019 last "DEFTECH pills" insightful and look forward to any feedback for continuous improvement.

We wish you a very good reading,

Tate Nurkin	Dr. Quentin Ladetto
OTH Intelligence Group	armasuisse S+T
CEO	Research director – Technology Foresight
tate.nurkin@othintel.com	quentin.ladetto@armasuisse.ch

Introduction and Summary

The final DEFTECH volume of 2019 covers a particularly busy period for the announcement and demonstration of new and emerging military capabilities. The DSEi (September) and AUSA (October) defence exhibitions were held during the reporting period (among other regional events). So, too, was the military parade associated with the 70th anniversary of the establishment of the People's Republic of China. This report has a strong focus on activities around these three events, but it also seeks to expand this focus and emphasize reporting on other novel (and in some cases lower profile) technologies and capabilities advanced or demonstrated in the United States, United Kingdom, Austria, Russia, China, and Turkey.

Two broad insights about the intersection of emerging technologies and military capabilities derived from developments in and across each of the categories of capabilities include:

Framing and Prioritising Emerging Technology Investment: The pace of innovation and breadth of technologies of interest to military communities is increasingly forcing defence and security communities of all sizes to think through their approaches to military technology and innovation and formally create frameworks and policies to govern prioritisation, investment and deployment of these technologies. For example, the United States Department of Defense (DoD) released its ethical principles for artificial intelligence (AI) in early November 2019 while in September 2019, the United Kingdom Ministry of Defence published both its Defence Technology Framework and Defence Innovation Priorities.

Together the UK papers establish a strategic technology roadmap and outline the investment plans for the MoD in seven families of technologies that are likely to have the biggest impact for the UK MoD: 1) advanced materials; 2) artificial intelligence, machine learning and data science; 3) autonomous systems and robotics; 4) power, energy storage, conversion, and transmission; 5) sensors; 6) advanced electronics and computing; 7) effector technologies. The two documents also stress the need for a more collaborative relationship with the global defence and high-tech industry and more investment in UK small and medium enterprises, a regular theme covered by the DEFTECH report.

Capabilities and Technologies: Developments in the reporting period revealed that the discussion of military-technology and future military capabilities is increasingly complicated by a lack of precision in language, specifically the tendency to conflate the terms–or at very least the concepts--'technology' and 'capability'.

Inventions in technologies expand the scope and scale of what is possible from an engineering or physics standpoint. However, invention of a technology does not constitute the development of a capability, which itself is only a conduit to achieving an effect as demonstrated in the figure below. For both large and small militaries, the process of prioritizing technological investments should begin first with the effect that the military needs to achieve and then proceed to a thorough review of how the combination of advanced technologies and emerging operational concepts, doctrine, procurement processes, and other non-technical innovations can best achieve that effect.

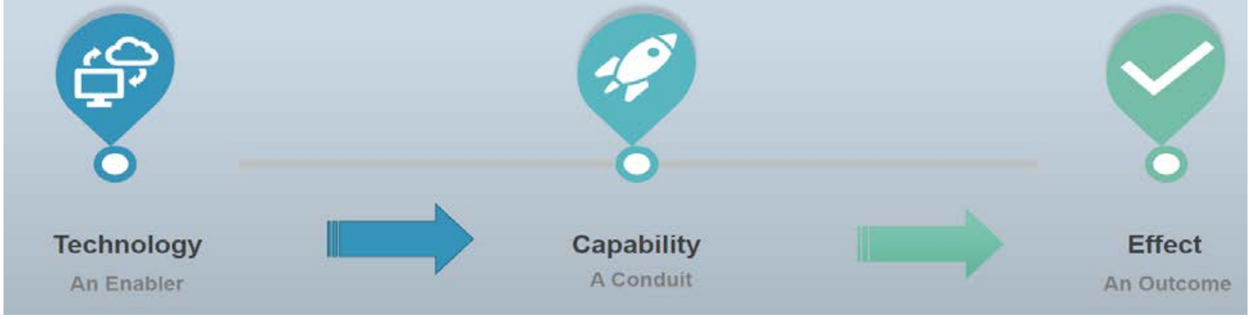


Figure 1: A spectrum of innovation and development, from technology to capability to effect (source: OTH Intelligence Group)

Energy, Power, and Propulsion

Key Insights:

- Attempts to make hydrogen fuel cells more efficient and to reduce costs of associated specialized infrastructure are maturing. The U.S. Army is already incorporating the rocket fuel additive Alane, which is lighter and more dense than compressed gas hydrogen, into multiple U.S. Army programs, including a wearable power system that is undergoing testing.
- Scaling the production of Alane (and feasibly other similar unconventional energy sources) remains a key challenge, **but for small militaries there may be opportunities for focused and specific use to enhance specific critical mission capabilities**
- **Wearable / individual soldier fuel cells** are another in-demand application of fuel cell technology as individual soldiers carry more advanced electronics equipment as part of their standard kit

Rocket Fuel Additive: Reporting from *Defense One* in September 2019 highlighted the growing interest of the U.S. Army in the development of aluminium hydride—AIH3 or Alane—a compound originally developed in the 1970s as an additive to rocket fuel. Alane could provide a "stable, energy dense key to unlocking a wide new range of power-hungry applications."[1]

Previous volumes of this report have focused on hydrogen fuel cells and the increased investments in this technology by both militaries and the commercial sector to generate more efficiency and endurance and lower the cost of operations of both manned and unmanned platforms. As much progress has been made in the development of hydrogen fuel cells in the last several years, challenges remain related to moving and storing "the universe's lightest element as a liquid or gas" as well as the volatility associated with compressed gas and liquid hydrogen.[2]

However, the *Defense One* report noted that Army investments in the material—which is described as looking "a lot like baby powder" and is "four times as energy dense as gaseous hydrogen"—are showing promise. Not only does Alane offer more energy than other sources, but it is also simultaneously lighter and denser and does not require special tanker trucks or pipelines to transport.

Contractor Ardica is currently working with the U.S. Army to develop a 20-watt wearable power system that is undergoing field testing in Army Expeditionary Warrior Experiments as well as a 300-watt generator. The former is expected to go into production "soon" while a prototype of the latter is expected "in six months".[3] Use of Alane to power vehicles is also under consideration as the cost of Alane development decreases.

[1] Tucker, Patrick, "A Rocket-Fuel Additive Could Be the Next Great Power Breakthrough", *Defense One,* 9 September 2019, https://www.defenseone.com/technology/2019/09/rocket-fuel-additive-could-be-next-great-power-breakthrough/159749/?oref=d-river

[2] Tucker, Patrick, "A Rocket-Fuel Additive Could Be the Next Great Power Breakthrough", *Defense One,* 9 September 2019, https://www.defenseone.com/technology/2019/09/rocket-fuel-additive-could-be-next-great-power-breakthrough/159749/?oref=d-river

[3] Tucker, Patrick, "A Rocket-Fuel Additive Could Be the Next Great Power Breakthrough", *Defense One,* 9 September 2019, https://www.defenseone.com/technology/2019/09/rocket-fuel-additive-could-be-next-great-power-breakthrough/159749/?oref=d-river

However, the report did note that the primary obstacle to broader use may well be production at the scale necessary to support the U.S. Army and broader DoD—estimated at 40,000 metric tons.[4]

In conjunction with the flurry of reporting on hydrogen fuel cells and lithium ion battery developments over the last several DEFTECH volumes, the Alane report highlights a common concern and opportunity for militaries throughout the world the need for scalable, stable, cost – efficient sources of energy to increase the endurance and efficiency of humans and platforms and the increasingly high-tech equipment and electronics that militaries rely on for operational success.

Indeed, *Warrior Maven* reported in August 2019 that Army Research Lab scientists are now working with Cornell University to manufacture new smaller, safer and more efficient electricity-generating fuel cells for use by soldiers in combat. This new effort seeks to create an entirely new fuel cell over the next five years that will replace hydrogen with methanol.[5]

Human Performance Enhancement

Key Insights:

- As new technologies become available and strategic and operational environments become more complex and multi-dimensional, **militaries around the world are reconsidering approaches to training**
- **There is a growing emphasis on blended training programs** that combine **live training** (which is typically expensive and brings in some safety concerns), **synthetic or simulated training** (which leverages novel technologies such as virtual and augmented reality, machine learning, and cloud computing), and **constructive class-room training**
- Another focus area of improving human performance for militaries of all sizes an**d budgets is the increasing incorporation of best practices for health and training from the world of high-performance sports.** This reporting period features reporting on the incorporation of "pre-habilitation" solutions by the U.S. Air Force Special Operations Command

Transformational Training in the United Kingdom: The UK Army is expected to release a request for information in early November to formally launch a competition that will fundamentally alter the way the Army in particularly conducts training. The initiative known as the Collective Training Transformation Program (CTTP) is part of the Army's new Future Collective Training System and is expected to "become a surrogate for warfare; driving adaptation, generating combat ethos, empowering commanders, an delivering tactical innovation."[6]

Key components of the program include: upgraded urban training facilities, additional virtual training at Army bases, and potential use of innovative synthetic training capabilities. Lockheed Martin UK, Babcock

[4] Tucker, Patrick, "A Rocket-Fuel Additive Could Be the Next Great Power Breakthrough", *Defense One,* 9 September 2019, https://www.defenseone.com/technology/2019/09/rocket-fuel-additive-could-be-next-great-power-breakthrough/159749/?oref=d-river

[5] Osborn, Kris, "Army Sets Sights on New Fuel Cell Technology" *Fox News,* 12 August, 2018, https://www.foxnews.com/tech/army-sets-sights-on-new-fuel-cell-technology

[6] Chuter, Andrew, "The UK is ready to kick off an effort to revamp military training", *Defense News,* 16 October 2019, https://www.defensenews.com/global/europe/2019/10/16/the-uk-is-ready-to-kick-off-an-effort-to-revamp-military-training/

International, and Raytheon UK have all confirmed their interest in the program, which is expected to have a budget of $770 million and achieve full operating capability by 2025.[7]

The UK program is indicative of a move toward "blended" training that incorporates enhanced live training with simulated or virtual training and constructive / classroom training. Demand among many militaries for this approach to training is driven by a range of prevailing forces, such as:

- A shifting and expanding threat environment that is reorienting toward conflict and competition between state actors rather than the largely counter-insurgency operations that have consumed the attentions of Western militaries for much of the last two - decades
- The emergence of a highly complex multi-domain battlefield, hybrid warfare threats, and emphasis on the urban battlefield that are difficult to simulate in live training or unsophisticated simulations
- The maturation of several emerging technologies, such as machine learning, cloud computing, virtual and augmented reality, among others that are making it easier and far less expensive to provide both constructive and virtual trainings at lower costs
- The need to quickly and efficiently move trainees through the training process in order to fill key capability gaps (pilots, for example) that are relatively consistent across small and large militaries. Blended training systems enable trainees to get a high-number of repetitions in low – cost settings before being rushed into more expensive and challenging training environments

The Continued Intersection between Sports and Soldier Performance Enhancement: The previous volume of this report included reporting on U.S. Army efforts to embed 55 "Master Resilience Trainers-Performance Experts" with Reserve Officer Training Corps in order to improve cognitive, psychological, and physical performance.[8] The effort is part of a larger trend within many militaries of various sizes across the world to leverage the best practices and training techniques of high performance athletes in order to improve the stamina, strength, cognition, and overall performance of soldiers. This theme was highlighted again during the current reporting period as the U.S. Air Force Special Operations Command (AFSOC) operationalized its new Performance Maintenance Pad (PMP) concept at Duke Field in Florida.

> *"Regular prehab and supervised corrective techniques will reduce the risk of injury. Injury prevention and performance enhancement is what we do."—Erin Jenkins, Preservation of the Force and Family's Human Performance Program at Duke Field*

The PMP consists of a physical therapist, athletic training, and two strength and conditioning coaches and focused on "pre-habilitation" to reduce the risk of injury associated with training and active duty. According to Sylvia Nelson, AFSOC's Force Resilience and POTFF Division Chief, "the ultimate goal of (the program) is to increase readiness of our Air Commandos by sustaining and improving physical, nutritional and cognitive performance, enabling rapid rehabilitation form injury and increasing their lethality and career longevity."[9]

[7] Chuter, Andrew, "The UK is ready to kick off an effort to revamp military training", *Defense News,* 16 October 2019, https://www.defensenews.com/global/europe/2019/10/16/the-uk-is-ready-to-kick-off-an-effort-to-revamp-military-training/

[8] Rico Antonieta, "Resilience experts aim to boost performance at ROTC camp", *U.S. Army,* 12 July 2019, https://www.army.mil/article/224468/resilience_experts_aim_to_boost_performance_at_rotc_camp

[9] Reeves, Major Amanda, "Duke Filed focusing on prevanttive health conditioning", 919 Special Operations Wing website, 19 September 2019, https://www.919sow.afrc.af.mil/News/Article-Display/Article/1965475/duke-field-focusing-on-preventative-health-conditioning/

Cyber and C4ISTAR

Key Insights:

- **Advances in artificial intelligence are creating new technology-driven capabilities that can be leveraged as part of disinformation, recruitment, theft, and election meddling campaigns.** Deepfakes and smart bots, in particular, have the capacity to create strategic political and societal disruptions or enhance fundraising and recruiting by non-state actors in more efficient, impactful, or difficult to detect ways than currently are available. These outcomes should be of concern to militaries and security communities of all sizes.
- A university in Austria successfully tested a **quantum radar** in August. **The technology does have the potential to change components of the hiding versus detection competition**, though statements that quantum radars will eliminate the value of stealthy platforms likely overstates the immediate effect of the technology. For small militaries, the new capabilities introduced by quantum radars will likely influence future decision making on the types of capabilities they procure and operational concepts they develop.
- **Offensive cyber capabilities are becoming more difficult to detect and attribute and are diffusing more broadly.** Military and security communities throughout the world are increasingly investigating various means of building resilience of critical military, civilian, and commercial infrastructure, including investigating means of reducing risk of cyber attacks on space infrastructure.

Artificial Intelligence Applications for the Information Warfare: Two examples of how different artificial intelligence applications are already being applied to support disinformation campaigns, information operations, and targeted coercion or theft were highlighted during the reporting period.

In September 2019, media outlets reported that audio deepfakes were applied by criminals to trick a UK energy company CEO into wrongly wiring €200,000 to a purported supplier in Hungary. The perpetrators were likely organized crime. The deepfake was used to imitate the sound of the CEO's boss' voice, "and not only the voice: the tonality, the punctuation, the German accent."[10] When the fake voice requested the payment be made, the CEO complied.

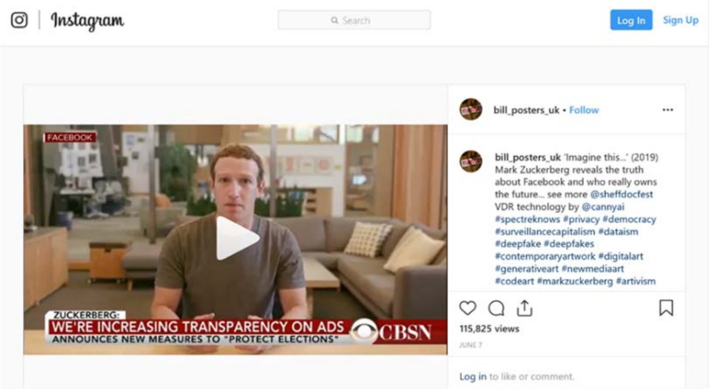
The use of a voice deepfake reflects the emerging challenges of artificial intelligence enabled tools of deception being deployed for a range of tactical, operational, and strategic effects that go well beyond theft. Recordings of world leaders making provocative or offensive statements, declaring war, or committing crimes could also be enabled by these technologies and particularly video or image deepfakes.

The erosion of the boundaries between the physical and digital world was also demonstrated in a study published in the journal *First Monday* and released in September 2019 that tracked how AI-enabled smart bots are growing more sophisticated and more human-like—making them more difficult to detect. The study reviewed 244,699 Twitter accounts that tweeted about politics or the 2016 and 2018 elections in the United States, determining that about 31,000 accounts were bots.

[10] Statt, Nick, "Thieves are now using AI deepfakes to trick companies into sending them money", *The Verge,* 5 September 2019, https://www.theverge.com/2019/9/5/20851248/deepfakes-ai-fake-audio-phone-calls-thieves-trick-companies-stealing-money)

More worryingly, the study also found a difference in the sophistication of the activity between 2016 and 2018—by 2018, “bots better aligned with humans’ activity trends, suggesting the hypothesis that some bots have growing more sophisticated.”[11] Bots also did less retweeting, reflecting a trend among human users of Twitter who are more focused on replies.[12] Overall, the report indicates that it is “increasingly difficult to distinguish between interactions with humans from those with machines deployed to manipulate, influence, and outrage targeted populations.”[13]

For militaries and security communities of nearly all sizes, efforts to weaponize social media are especially concerning in a world marked not only by the fusion of the digital and physical worlds, but also of reality and perception and by the rapid development and diffusion of advanced applications of artificial intelligence. In this environment, the study “further corroborates this idea that there is an arms race between bots and detection algorithms . . . Advancements in AI enable bots producing more human-like content.”[14]


Instagram
Search
Log In
Sign Up
FACEBOOK
ZUCKERBERG:
WE'RE INCREASING TRANSPARENCY ON ADS
ANNOUNCES NEW MEASURES TO "PROTECT ELECTIONS"
CBSN
bill_posters_uk • Follow

bill_posters_uk 'Imagine this...' (2019) Mark Zuckerberg reveals the truth about Facebook and who really owns the future... see more @sheffdocfest VDR technology by @cannyai #spectreknows #privacy #democracy #surveillancecapitalism #dataism #deepfake #deepfakes #contemporaryartwork #digitalart #generativeart #newmediaart #codeart #markzuckerberg #artivism

115,825 views

JUNE 7

Log in to like or comment.

Figure 1: In June 2019, a deepfake of Facebook CEO Mark Zuckerberg talking to CBS News about “the truth of Facebook and who really owns the future” was put on Instagram. The video is of reasonable quality, though the message the fake Zuckerberg delivers is clearly a tongue in cheek effort to draw attention to the increasingly urgent challenges for Facebook in particular of monitoring content and balancing content flows in the information age. Nonetheless, the footage along with deepfake footage of former President Obama delivering speeches he never gave and other examples of deepfake technology should catalyze defence and security communities of all sizes to begin to contemplate the detection and defeat of deepfakes

Significantly, the research was, according to *Defense One,* supported in part by the U.S. Air Force’s Office of Scientific Research, [15] further underscoring the importance of these applications of AI for defence communities and militaries.

> *The study “further corroborates this idea that there is an arms race between bots and detection algorithms . . . Advancements in AI enable bots producing more human-like content.”*

Quantum Radar Successfully Demonstrated: A quantum radar system was successfully tested for the first time on 23 August 2019 by researchers at Austria’s Institute of Science and Technology.[16] Previously, on 5 November 2018, China Electronics Technology Group Corporation’s (CETC) 14th Institute displayed a prototype of a quantum radar at the Zhuhai Airshow during a limited press conference for Chinese journalists. According to a CETC brochure distributed at the Airshow, the quantum radar “is expected to solve the traditional bottleneck (of) detection of low observable target detection, survival under electronic warfare conditions, platform load limitations, etc.”[17] It is certainly interesting and perhaps more than just coincidental that an Austrian university

[11] Lucerri, Luca, Ashok, Deb, Giordono, Silvia, Ferrara, Emilio, “Evolution of bot and human behavior during elections”, *First Monday,* 2 September 2019, https://firstmonday.org/ojs/index.php/fm/article/view/10213/8073

[12] Lucerri, Luca, Ashok, Deb, Giordono, Silvia, Ferrara, Emilio, “Evolution of bot and human behavior during elections”, *First Monday,* 2 September 2019, https://firstmonday.org/ojs/index.php/fm/article/view/10213/8073

[13] Lucerri, Luca, Ashok, Deb, Giordono, Silvia, Ferrara, Emilio, “Evolution of bot and human behavior during elections”, *First Monday,* 2 September 2019, https://firstmonday.org/ojs/index.php/fm/article/view/10213/8073

[14] Lucerri, Luca, Ashok, Deb, Giordono, Silvia, Ferrara, Emilio, “Evolution of bot and human behavior during elections”, *First Monday, 2 September 2019, https://firstmonday.org/ojs/index.php/fm/article/view/10213/8073*

[15] Tucker, Patrick, “Twitter Bots Are Becoming More Human-Like: Study”, *Defense One,* 6 September 2019, https://www.defenseone.com/technology/2019/09/twitter-bots-are-becoming-more-human-study/159697/

[16] Mizokami, Kyle, “How Quantum Radar Could Completely Change Warfare”, *Popular Mechanics*, 26 August 2019, https://www.popularmechanics.com/military/a28818232/quantum-radar/

[17] Trimble, Steve, “China Shows Off First Quantum Radar Prototype”, *Aviation Week,* 5 November 2018, **http://aviationweek.com/defense/china-shows-first-quantum-radar-prototype**

has developed this technology, given previous collaboration on quantum encryption between China's Academy of Sciences and the Austrian Academy of Sciences.

Interest in quantum radars is rooted in the several perceived advantages these radars bring, namely:

- Increased accuracy / definition and detail of identification. Rather than merely identified an object and its general parameters and specifications, quantum radars will provide the ability to identify specific platforms
- Much of the literature about quantum radars stress a supposedly "game-changing" capacity to detect stealthy aircraft. And while quantum radars should enhance the ability to detect stealthy aircraft, many observers do not believe that the incorporation of quantum radars will eliminate the value of stealth. Instead, they will introduce a next phase in the competition between attempts to hide aircraft / missiles and detect them.[18]
- Quantum radars are themselves relatively stealthy and hard to detect, meaning that they are able to operate without a high-risk of attempted interference and are considered to be resistant to efforts to jam

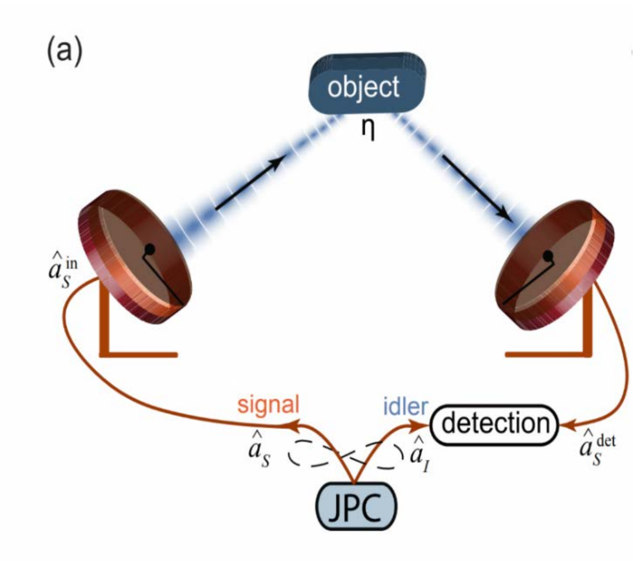


Figure 2: The concept behind the successfully tested quantum radar (MIT Technology Review)

The Cyber Conflict: The reporting period once again saw considerable reporting on new developments in both offensive and defensive cyber capability.

On 22 October 2019, a joint advisory from the U.S. National Security Agency and UK National Cyber Security Centre warned that cyber-group Turla, widely believed to be Russian, co-opted two Iranian hacking tools known as "Nautilus" and "Neuron" in order to target military, government, academic, and scientific organizations in at least 35 different countries.[19]

The notice indicated that the tools had "very likely" been acquired by 2018 through a range of mechanisms, including scouring the networks of victims of the two tools for backdoors inserted by Iranian hackers. According to the advisory, "The timeline of incidents, and the behaviour of Turla in actively scanning for Iranian backdoors, indicates that while Neuron and Nautilus tools were Iranian in origin, Turla were using these tools and accesses independently to further their own intelligence requirements." Iranian hackers "were almost certainly not aware of, or complicit with, Turla's use of implants."[20]

[18] Mizokami, Kyle, "How Quantum Radar Could Completely Change Warfare", *Popular Mechanics*, 26 August 2019, https://www.popularmechanics.com/military/a28818232/quantum-radar/

[19] Corrigan, Jack, "Russian Hackers Co-Opt Iranian Cyber Tools to Attack 35 Countries, NSA Warns", *NextGov,* 22 October 2019, https://www.nextgov.com/cybersecurity/2019/10/russian-hackers-co-opt-iranian-cyber-tools-attack-35-countries-nsa-warns/160756/

[20] Corrigan, Jack, "Russian Hackers Co-Opt Iranian Cyber Tools to Attack 35 Countries, NSA Warns", *NextGov,* 22 October 2019, https://www.nextgov.com/cybersecurity/2019/10/russian-hackers-co-opt-iranian-cyber-tools-attack-35-countries-nsa-warns/160756/

Earlier, on 9 September 2019, reports emerged that a Chinese cyber-espionage group known as Thrip that Symantec first exposed in June 2018 may actually be part of another group that was discovered a decade ago.

> *"[The hackers] pause, retool, regroup and then they continue their mission" – Vikram Thakur, a technical director at Symantec*

Thrip reportedly has attacked targets in 12 organizations in Hong Kong, Macau, Indonesia, Malaysia, the Philippines, and Vietnam. Perhaps more importantly than its geographic focus, however, has been its learning capacity. According to Symantec, "When [Thrip] came back in October [or] November, we see [Thrip] using a brand new tool which is built from scratch [that] we've never seen before. [The hackers] pause, retool, regroup and then they continue their mission."[21]

Analysis of a backdoor the group has used, known as Sagerunex, reveals that Thrip is likely not an independent group, but associated with another Chinese group known as Billbug or Lotus Blossom, which has been operating against South Asian targets for years. Symantec was unable to determine the nature of the infection vector or attack vector related to the attacks against Southeast Asian military organizations, satellite communications operators, maritime communications organizations, and media.[22]

The reporting on these two threats offers another reminder for military and security communities of the growing complexity of the global cyber threat environment and the ability of sophisticated actors to not only leverage the tools of other hacking groups, but also to learn, adapt, and re-emerge in ways that can confuse even well-informed observers. Such an environment places a premium on threat identification and tracking as well as on effective counter measures to first detect and then protect critical military assets and physical and digital infrastructure as well as civilian and commercial organizations.

> *"It absolutely is possible to conduct cyber attacks against satellites. Satellites and their ground systems are increasingly just computers running some specialized software, but they often run common OSes like Unix or Linux. They are vulnerable to many of the same cyber attacks as every other computer system out there."— Brian Weeden, Director of Program Planning for Secure World Foundation*

For example, researchers at the National Security Agency in the United States are now employing artificial intelligence to identify and characterize anomalous behaviour in small satellites and potentially detect if these satellites have been secretly hacked. Russia tested another, admittedly much starker, approach to cyber resilience during the reporting period.[23]

On 1 November, Russia began tests of its internal RuNet to determine whether the government can function without access to the global internet. According to Russia analyst Samuel Bendett, "The larger context is Russia's dependence as a nation on imported / foreign hi-tech and the perceived vulnerabilities that Russia sees in such technology use. With so many government, public, and private-sector nodes using such foreign tech, the Russian government is seeking to impose a measure of control over how Internet communication over this technology is conducted."[24]

[21] Vavra, Shannon, "Symantec finds that a 'new' Chinese hacking group has actually been around for a decade", *CyberScoop / Computer Week,* 9 September 2019, https://www.cyberscoop.com/thrip-lotus-blossom-symantec-china/

[22] Vavra, Shannon, "Symantec finds that a 'new' Chinese hacking group has actually been around for a decade", *CyberScoop / Computer Week,* 9 September 2019, https://www.cyberscoop.com/thrip-lotus-blossom-symantec-china/

[23] Tucker, Patrick, "The NSA Is Studying Satellite Hacking", *Defense One,* 20 September 2019, https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/

[24] Tucker, Patrick, "Russia Will test Its Ability to Disconnect from the Internet", *Defense One,* 24 October 2019, https://www.defenseone.com/technology/2019/10/russia-will-test-its-ability-disconnect-internet/160861/

Manned Platforms

Key Insights:

- **Speed, endurance, survivability, reduction of pilot cognitive and physical burden, and flexibility of payloads** continue to be highly-prioritized attributes for manned platforms as new technologies such as new means of propulsion and energy capture, storage, and distribution; enhanced autonomy; smart sensors and materials; and human-machine teaming are integrated into platform design and operational concepts
- Rapid advancements in these technologies and shifts in the security environment are forcing militaries of all sizes and postures **to consider new means of engaging and buying from industry** that increase the ability of defence communities to integrate new capabilities quickly and adapt to new strategic and operational environments
- **Deepening intersection of commercial and traditional defence industry priorities and capabilities** is driving more engagement between defence industry companies and adjacent industries, such as automotive, commercial aerospace, and commercial high-tech

New Development and Procurement Models: The reporting period saw in two U.S. DoD programs that are attempting to leverage novel approaches to the development and procurement of high-tech enabled next generation capability.

At the AUSA defence exhibition in Washington, DC in mid-October both Sikorsky and Karem revealed their designs for the Army's Future Attack Reconnaissance Aircraft (FARA) program. The two design reveals follow closely on a similar announcement from Bell in early October. These are three of the five competitors down selected in April for the competition. AVX / L-3 showed their design earlier in the year. The fifth competitor, Boeing, has yet to reveal its design.

Figure 2: An artist rendering of the Bell 360 Invictus being offered to the U.S. Army as part of the FARA competition (source: Defense News)

The competition seeks to provide the U.S. Army with a high-speed, high-endurance aircraft capable of penetrating contested airspace (especially in urban environments) to carry out a range of missions, from strike and air-space control to forward air control to electronic warfare attack.

FARA is notable not only for the novel technologies being applied to the rotary wing aircraft, such as increased autonomy, fly-by-wire, co-axial blades, and advanced material, but also for the process through which the procurement is being run. The Army has moved quickly—it was reportedly two months ahead in its down-select decision in April—and expects to select two competitors to move to the prototype stage in early 2020 with an objective of choosing a single platform by 2023 and final delivery by 2028.[25]

The program is also of interest because while it lays out broad requirements for the end capabilities of the aircraft, it does not prescribe how industry should design the aircraft to achieve these capabilities. To date, this approach appears to have catalysed innovation from the four competitors that have revealed their designs. Each has taken a different approach stressing different technologies, value propositions, and means of achieving the broad performance parameters laid out by the Army.[26] The result is that the U.S. Army now has clearly differentiated options for achieving its hoped-for disruptive effects.

In addition, on 22 October, the U.S. Air Force's Assistant Secretary for Acquisition, Technology, and Logistics made comments at an Aviation Week forum that the Air Force is adjusting its plans for the Next-Generation Air Dominance (NGAD) program.

The program was originally designed to develop a replacement for the F-22 by 2030, and options for a next generation F-X fighter were investigated. But the Air Force has now adjusted to a more radical approach to future aircraft development. According to Roper, "it's a good time to try something new for a five-year window and see if we can create a new way to build airplanes for us that [is] between the building of one or two X-planes and the building of 1,000 units in a major defence acquisition program."[27]

The model posited by Roper is closer to the one for consumer electronic devices in which consumers buy an iPhone model designed to become obsolete in a few years rather than a traditional military program designed to create a program expected to survive and be upgraded for decades. According to *Aviation Week* the equivalent model for the fighter business involves "aircraft designed to last perhaps 3,500 flight hours, which the U.S. Air Force buys in batches of hundreds and replaces in intervals of 10 years or less." A key objective of this program is to get smaller and non-traditional defence firms more involved in the development and delivery of fighter jets.[28]

Together, these two programs demonstrate dynamics that go well beyond the U.S. and other large militaries as defence and security communities attempt to cope with the expanding military applications of the innovation in Fourth Industrial Revolution technologies, many of which are being developed outside of the traditional defence sector. This environment is placing a premium on the ability to move quickly to incorporate new technologies and the new capabilities they enable. In many cases, this requires a reimagining of how defence communities engage with and buy from a global defence industry that is increasingly intersecting with adjacent commercial industry and applied research centres.

Porsche and Boeing Partner: One example of the deepening relationships between the traditional aerospace and defence industry and other adjacent commercial industries is seen in the announcement on 18 October that Boeing and Porsche along with Boeing subsidiary Aurora Flight Sciences have signed a memorandum of understanding (MoU) to jointly explore the "premium" electrical vertical take-off and landing aircraft market.[29]

[25] Tadjdeh, Yasmin, "Army's Future Attack Recon Aircraft Gains Momentum", *National Defense,* 9 October 2019, https://www.nationaldefensemagazine.org/articles/2019/10/9/armys-future-attack-recon-aircraft-gains-momentum

[26]Tadjdeh, Yasmin, "Army's Future Attack Recon Aircraft Gains Momentum", *National Defense,* 9 October 2019, https://www.nationaldefensemagazine.org/articles/2019/10/9/armys-future-attack-recon-aircraft-gains-momentum

[27] Trimble, Steve and Hudson, Lee, "USAF Sees Five-Year window To Invent a New Fighter Aircraft Industry", *Aviation Week*, 29 October 2019, https://aviationweek.com/defense/usaf-sees-five-year-window-invent-new-fighter-aircraft-industry

[28] Trimble, Steve and Hudson, Lee, "USAF Sees Five-Year window To Invent a New Fighter Aircraft Industry", *Aviation Week*, 29 October 2019, https://aviationweek.com/defense/usaf-sees-five-year-window-invent-new-fighter-aircraft-industry

[29] Zart, Nicolas, "Porsche & Boeing Sign An Agreement To Work On "Premium" eVTOL Aircraft", *CleanTechnica,* 18 October, 2019, https://cleantechnica.com/2019/10/18/porsche-boeing-sign-an-agreement-to-work-on-premium-evtol-aircraft/

Press-releases from both companies stress the partnership's focus on meeting to better understand opportunities created by the extension of urban traffic into airspace and the changing landscape of urban mobility. However, the development of a high-end transport craft (either manned or unmanned) that can efficiently move people and cargo across large distances or, plausibly, urban areas will have relevance for military and security communities.

Missile Systems and Munitions

Key Insights:

- **The People's Republic of China celebrated the 70th anniversary of its founding with a large military parade** that provided insight into many of the advanced capabilities, especially weapons systems, that it has developed over the last several years.
- Among the systems displayed were the **DF-17 hypersonic glide vehicle** and **DF-41 road mobile ICBM** as well as the JL-2 sub-launched ballistic missile.
- The increased maturity of the **DF-17** weapon is particularly notable and **reflects the faster-than-expected advancement of hypersonic weapons touched on in previous volumes of this report.** For large and small militaries, the rapid advancement of both glide vehicles and air-launched weapons are introducing new and potentially disruptive dynamics into the strike versus air and missile defence competition.
- **Directed energy weapons continue to be a focus of both large and small militaries** as Turkey successfully completed testing on its vehicle mounted directed energy system during the reporting period. These weapons are already being used to perform several military missions and are likely to diffuse relatively rapidly

China's Missiles on Display: Two much – anticipated advanced weapons systems were revealed during the military parade associated with the 70th birthday of the People's Republic of China.

The introduction of the DF-17 hypersonic glide vehicle, which was paraded carrying a ballistic missile, stood out as particularly provocative and impressive and indicates the continued global progress on hypersonic flight and the advanced materials and communications systems and flight controls required to manoeuvre a weapon traveling over Mach 5. It will also no doubt inspire continued investments from the United States both in hypersonic weapons development and hypersonic defence.

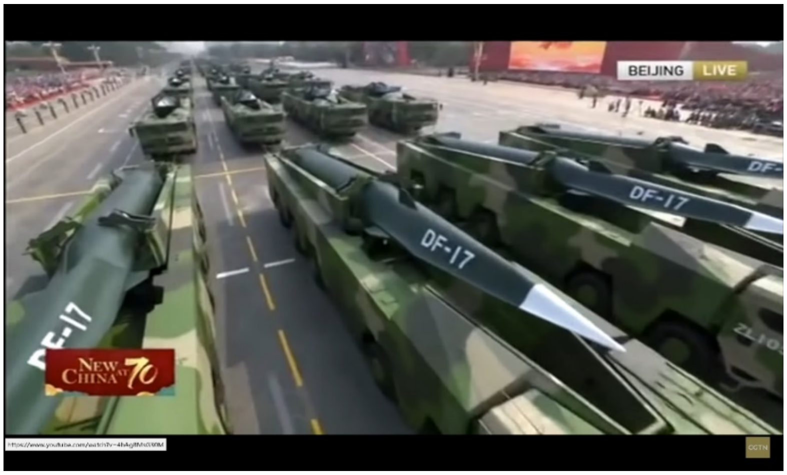


Figure 3: The DF-17 on display during the 70th Anniversary of the founding of the PRC on 30 September 2019. Source: YouTube

Tracking this competition—which took a critical step forward during the parade—will offer some insight for smaller militaries that have not prioritized hypersonic weapons development into the direction of technology and operational concept development in hypersonic weapons, especially the more exquisite technologies associated with hypersonic glide vehicles (as opposed to air-launched hypersonic weapons). According to reporting on the parade, the announcer noted that the DF-17 is expected to have a conventional payload, though the U.S. military does believe the missile will be nuclear capable.

The parade concluded with the DF-41 Intercontinental Ballistic Missile (ICBM). The DF-41 is the most advanced of the DF series and is a road mobile, ICBM capable of carrying multiple independently targetable re-entry vehicles. Its road mobile capability is especially important, offering a high degree of survivability during conflict and also offers more flexibility to respond to fast moving perceived threats as required. According to coverage of the parade from *The Diplomat,* "The DF-41 is expected to become the cornerstone of China's strategic deterrence."[30]

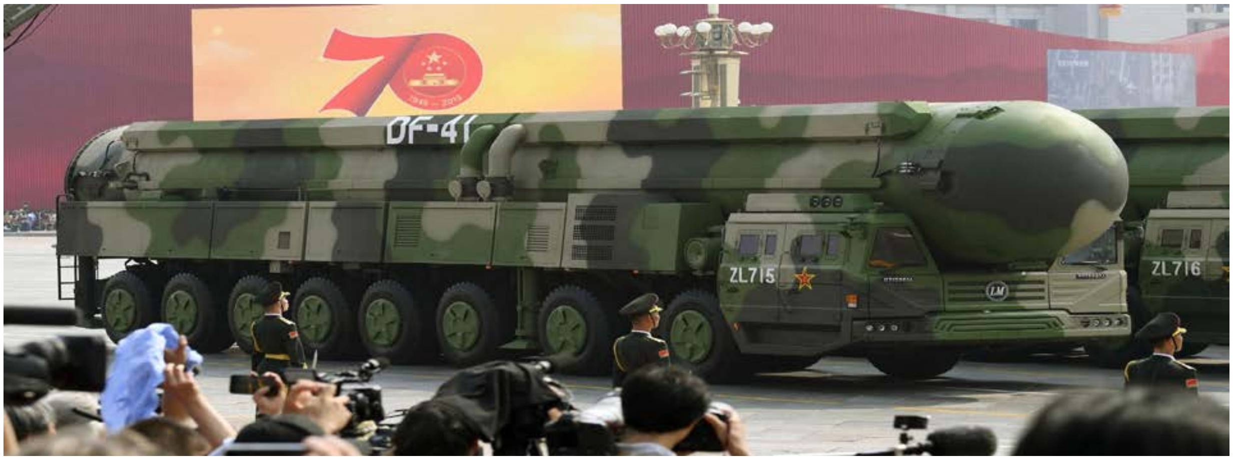


Figure 4: The DF-41 on display at the 70th Anniversary parade (Source: CCTV)

More on Directed Energy: A 2 October 2019 press release from the Informatics and Information Security Research Centre (BILGEM) of Turkey's Scientific and Technological Research Council claimed that the Vehicle-Mounted Laser System (ARMOL) has successfully completed acceptance tests. This is the first directed energy weapon to enter service with the Turkish Armed Forces.

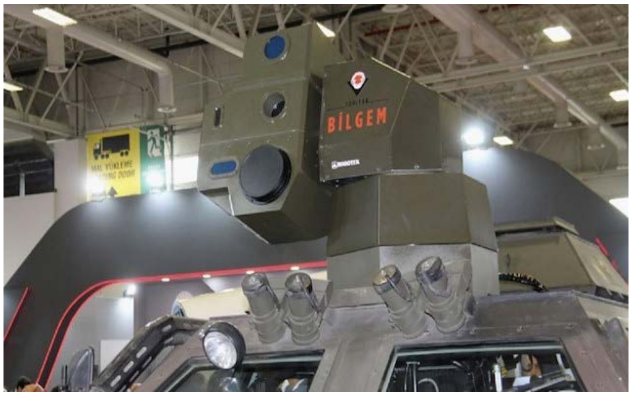


Figure 5: The BILGEM developed ARMOL system (source: Jane's)

According to the press release: "ARMOL, together with its high-powered laser system, is capable of taking high-resolution images outdoors. With this feature, it provides the opportunity to gather information for intelligence purposes, to identify threats in advance, and to make the necessary plans in advance for the inactivation process."[31]

Militaries throughout the world are increasingly developing a growing range of directed energy weapons and deploying them to carry out a range of defence and security-related missions:

[30] Panda, Ankit, "A Modern, Advanced People's Liberation Army: First Takeaways From the 70th Anniversary Parade", *The Diplomat,* 2 October 2019, https://thediplomat.com/2019/10/a-modern-advanced-peoples-liberation-army-first-takeaways-from-the-70th-anniversary-parade/

[31] Sarilbrahimoglu, Lale, "Turkish laser weapon passes acceptance test", *Jane's 360,* 4 October 2019, https://www.janes.com/article/91706/turkish-laser-weapon-passes-acceptance-tests

- Surveillance and target acquisition / detection
- Dazzling of satellites
- Jamming of navigation and communication systems
- Counter-drone missions
- Close – in and fixed installation defence
- Active protection systems

Robotics and Unmanned Systems

Key Insights:

- **New low-tech concepts are being incorporated to help solve many of the most pressing challenges for optimizing unmanned systems.** The use of tethers to increase persistence of small UAVs is a useful example, though in many cases the incorporation of these novel solutions come with trade-offs in terms of mission flexibility or performance
- **The push for more autonomous unmanned systems** is accelerating and increasingly providing value largely by replacing humans in carrying out dull and dangerous missions more efficiently and more safely than humans could. Replacing humans is just one level of how AI is proving value to militaries around the world—large and small. AI-enabled capabilities also are supporting humans and exceeding humans.
- **Stealthy drone development** is continuing apace with implications for large militaries, of course, but also smaller militaries that must increasingly organize for an operational environment over the next five plus years in which these technologies will have diffused

Tether Kits for Drones: FLIR Systems has developed a tether kit that can dramatically increase the endurance of its SkyRanger R70 and R80D SkyRaider small unmanned aerial vehicles (UAVs). The tether is an interesting relatively low-tech solution to the on-going challenge of maximizing endurance of even small unmanned systems that face both small and large militaries throughout the world.[32]

The tether will be used to supply continuous power to the UAV, enabling it to stay aloft for up to 24 hours rather than for less than one-hour with battery powered free flight.[33] Obviously, by tethering the UAV to a fixed point on the ground, the concept trades mobility for endurance, however, given the short flight times of an untethered system it appears the concept will enhance overall operational utility. FLIR envisions tethered UAVs as being particularly useful in persistent surveillance over fixed positions and as a communications relay that is less expensive and unwieldy than sensor-equipped towers.

US Navy Autonomous Milestone: The United States Navy reached a major milestone in its efforts to autonomously combat mines in September 2019. The Navy successfully demonstrated single-sortie mine

[32] Sellinger, Marc, "FLIR to unveil tether kit for drones", *Jane's 360,* 4 October 2019, https://www.janes.com/article/91710/flir-to-unveil-tether-kit-for-drones

[33] Sellinger, Marc, "FLIR to unveil tether kit for drones", *Jane's 360,* 4 October 2019, https://www.janes.com/article/91710/flir-to-unveil-tether-kit-for-drones

hunting in which an autonomous boat is able to sweep for mines, detect a mine-like object, classify it, and then deploy another system to destroy the mine.[34]

This capability is considered a significant enabler of efficiency and safety in a critical mission for navies and coastal or riverine protection forces throughout the word. Mine clearing has typically been a time-consuming process that involved the iterative deployment of divers to detect and dispose of the growing menace of low-cost mines. By transitioning to a fully machine-driven process, this technology will not only speed up mine-clearing, but also increase safety by removing people from the process.

Sharp Sword Stealthy UAV: China revealed a new model of the Sharp Sword stealth UAV (designated GJ-11) during the 70th anniversary parade. The new model includes several design modifications, including a "completely redesigned rear aspect with a stealthier exhaust compared to an earlier prototype that could significantly improve the unmanned aircraft radar-evading capabilities."[35]

Narrators of the parade indicated the Sharp Sword will be used largely for deep penetrating strikes, a mission profile indicated by its "GJ" designation, which stands for "gonji" or "attack" in English.[36]

Assessments of the version on display also indicated that it was actually a model of a still developing variant as it lacked several features expected to be on a flying aircraft. Nonetheless, the display of the GJ-11 during China's most high-profile and watched military parade does indicate the continuing prioritization of the development of stealthy UAVs, an area that Russia is pursuing as well.[37]

While the Sharp Sword (and many weapons on display during the parade) is typically viewed through the prism of U.S.-China competition, this overall continued focus on stealthy UAVs and UAVs more broadly should be of interest for small militaries throughout the world much in the same way that hypersonic glide vehicles should be. These are technologies and capabilities that are likely to move quickly and to become viable military capabilities in the next five years. They are also likely to diffuse, meaning that militaries will need to develop means of possibly acquiring their own capabilities as well as technology-enabled capabilities and operational concepts to meet any perceived challenges posed by increased development of stealthy unmanned systems.

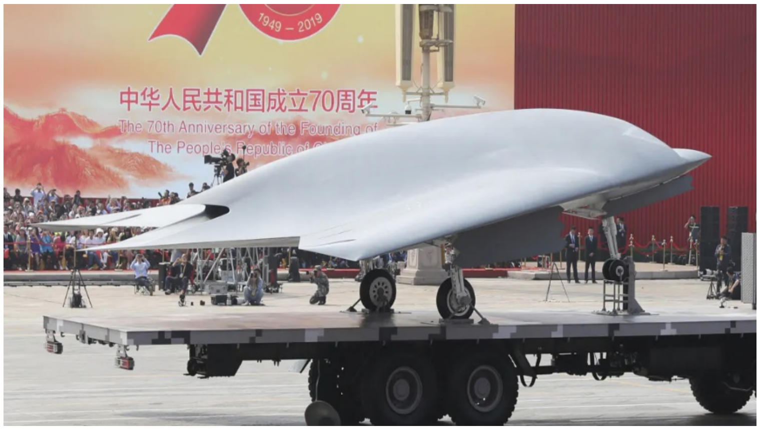


Figure 6: The new configuration of the Sharp Sword stealthy UAV (source: The Drive)

[34] Larter, David, "US Navy Makes Major Breakthrough in Autonomous Weapons", *Defense News,* 10 September 2019, https://www.defensenews.com/digital-show-dailies/dsei/2019/09/10/the-us-navy-just-had-a-major-breakthrough-with-autonomous-weapons/

[35] Trevithick, Joseph, "China Showcases Stealthier Sharp Sword Unmanned Combat Air Vehicle Configuration", *The Drive,* 1 October 2019, https://www.thedrive.com/the-war-zone/30111/china-showcases-stealthier-sharp-sword-unmanned-combat-air-vehicle-configuration

[36] Trevithick, Joseph, "China Showcases Stealthier Sharp Sword Unmanned Combat Air Vehicle Configuration", *The Drive,* 1 October 2019, https://www.thedrive.com/the-war-zone/30111/china-showcases-stealthier-sharp-sword-unmanned-combat-air-vehicle-configuration

[37] Trevithick, Joseph, "China Showcases Stealthier Sharp Sword Unmanned Combat Air Vehicle Configuration", *The Drive,* 1 October 2019, https://www.thedrive.com/the-war-zone/30111/china-showcases-stealthier-sharp-sword-unmanned-combat-air-vehicle-configuration

armasuisse

Inspire

Inform Instruct

DEFTECH

Defence Future

Technologies

Science + Technology

https://deftech.ch