Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

deftech.scan

February 2024

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

https://deftech.ch/scans

deftech
defencefuturetechnologies

Dear Reader,

Welcome to the first Deftech-Scan edition of the year !

For the one of you used to the previous version, you will see a very small change in the naming of the different trends we are considering. The reason is that we are trying to build a coherent technology ecosystem between different projects and stakeholders. The new structure can be found here – https://deftech.ch/lfp .

The Deftech-Scan reports will not cover every trend in each release, as some other projects might address them more extensively, but we hope to provide a good overview of facts that impact the present with a foreseeable effect on the future!

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

We wish you an interesting read.

Foresightly Yours,

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

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

1. Applications of AI and data

1.1	**Scale AI to investigate large language models (LLMs) for defence** The U.S. Department of Defense (DoD) announced the contract award on the opening day of a conference hosted by the DoD's Chief Digital and AI Officer (CDAO) (source and source) *Assessment:* On 20 February, the DoD's CDAO announced it had selected California-based Scale AI to test and evaluate the uses of generative AI for military and defence applications. In a statement, Alexandr Wang, the founder and chief executive of Scale, said the company was "honoured to partner with the DoD" and stressed the importance of testing and evaluation of generative AI to help "understand the strengths and limitations of the technology, so it can be deployed responsibly." The announcement came on the opening day of a conference hosted by CDAO in Washington, DC that featured discussion of the risks and opportunities generative AI presents. High-level insights on DoD's approach to generative AI include: • DoD is interested in understanding the range of applications for generative AI and LLMs • Concerns remain over the propensity of LLMs to "hallucinate", or make-up facts and information, and the ability to manage this risk in a real-world environment in which individuals are asked to rapidly discern between accurate and inaccurate LLM outputs • There are also concerns about more intentional efforts by adversaries to access and corrupt underlying data sets so that LLMs put out wrong or damaging information that will reduce the quality of decision-making • Craig Martell, the chief digital and AI officer of DoD, told the conference that the incorporation of generative AI in DoD will rely on commercial solutions rather than solely on purpose-built DoD solutions. Nonetheless, Commodore Rachel Singleton, head of Britain's AI Center, noted at the conference that Britain did develop an internal and customized LLM solution to stop personnel from using commercial LLMs, reflecting persistent concern over data security challenges of commercial models

1.2	**"Constant stare": AI to improve indicators and warnings in the Indo-Pacific** Admiral Sam Paparo advocated for a "constant stare" capability in and over the contested territorial waters of the Indo-Pacific and the use of AI algorithms to better determine when a grey zone activity such as a military exercise is really a precursor to invasion (source) *Assessment:* As China engages in increasingly provocative behaviour in and around contested territorial waters in the South and East China Seas, it has become more difficult for intelligence analysts and decision-makers to fully decipher a particular action's intent. During a conference hosted by the U.S. Defense Innovation Unit (DIU) in Silicon Valley in February, Adm. Paparo stated that the increase in the size of Chinese forces involved in military exercises or maritime militia and coast guard actions has raised "the threshold for warning . . . Soon we'll be at a point where a force sufficient to execute a profound military operation is in the field and operating under a fig-leaf of exercise." This growing inability to "derive enemy intentions" or "would be intentions" is eroding strategic, operational, and tactical warning times. To combat this vulnerability, Adm. Paparo recommended the deployment of a large number of low-cost, long-endurance, attritable or expendable uncrewed aerial systems (UAS), uncrewed surface vehicles (USVs), and uncrewed underwater vehicles (UUVs) to persistently observe sensitive areas. This "constant stare" of surveillance assets will be able to collect huge amounts of complex data sets, which can then be interpreted by AI algorithms much more rapidly and accurately than humans, potentially seeing underlying patterns or anomalies that would indicate either an imminent operation or standard exercise.

1.3	**Strategic partnerships, technology innovation, and the dynamic nature of digital learning environment market** The British Army selected the team of BAE Systems and UK-based AI specialist Obrizum to develop a new tailorable Digital Learning Environment (DLE) that incorporates the latest in a fast moving technology area (source) *Assessment:* The team will use Obrizum's AI-powered adaptive learning technology to develop tailored training experiences for the British Army. The two companies believe the use of Obrizum's personalisation engines, high-fidelity Extended Reality (XR) technology and its diagnostic analytics, could offer improvements, efficiency, productivity, and risk identification. The DLE will also include virtual assistant technology and an AI-powered digital content store, enabling the British Army to adopt it according to their changing needs. Lucy Walton, head of training for BAE Systems' Air sector, captured the dynamism of the training market and need for even successfully primes to partner with emerging technology companies as innovations in new immersive and AI technologies has increased the accessibility, realism, and utility of digital learning environments. According to Walton, the partnership puts the company "in a unique position to understand the need to constantly evolve the training solutions we offer."

2. Robotics and Autonomous Systems

2.1	**France orders XLUUV submarine drone demonstrator** The contract with Naval Group is a follow-on to a May 2023 contract that studied the main use cases and system architectures for an uncrewed combat underwater vehicle (UCUV). The program will use Naval Group's XLUUV demonstrator as a testbed for integration of technologies and operational concepts (source and source) *Assessment:* On 28 December, France's Defence Procurement Agency (DGA) awarded Naval Group a contract to design, produce, and test a UCUV. A first follow-on contract was also reportedly signed for the design and customized development of Naval Group's Autonomous Decision-Making Process (ADMP) and secure autonomous navigation. DGA is seeking a long-endurance demonstrator with a length of more than 10 meters and weighing more than 10 metric tons, it said in a statement on 30 January. The project will allow the French Navy to "evaluate a new naval capability that could provide a medium-term operational response to new areas of conflict and asymmetric combat", according to Naval Group. Specifically, the demonstrator will assist in assessing whether underwater drones will be able to defend France's coast and underwater infrastructure from a growing range of threats. Two existing components of Naval Group's efforts to develop UUVs will be vital to the 24-month contract. First, Naval Group's self-funded XLUUV Demonstrator will serve as the testbed for the evaluation of new technologies as they are developed, theoretically speeding the process and ensuring the program stays on schedule and within budget. The vessel completed sea qualification at the end of the summer of 2023. Second, Naval Group will develop a customized version of its ADMP that will be designed to strengthen mission planning and monitoring and secure surface and underwater navigation, functions crucial for undersea operations and endurance. Naval Group developed ADMP—the brains of Naval Group UUV autonomy—to ensure its UUVs could carry out missions without having to be remote controlled. France is one of only a handful of countries currently developing XLUUVs—including the UK, US, China, Russia, South Korea, and Australia—though the undersea domain has become more crowded and important in recent years. While only a select group of countries are building large UUVs, more are focusing on the development and use of both crewed submarines and smaller UUVs for monitoring the undersea environment for military and asymmetric threats to undersea assets such as communication cables and energy pipelines.

2.2	**More on large autonomous underwater vehicles and Anduril's momentum** In February, U.S.-based company Anduril was selected by the Defense Innovation Unit (DIU) to prototype a distributed, long-range, persistent underwater sensing and payload delivery large autonomous underwater vehicle (AUV) for the United States Navy. Anduril began as a software company but has gained momentum in building uncrewed systems (source and source) *Assessment:* As with the Naval Group development effort, Anduril's support will leverage and adapt existing Anduril hardware and software solutions to meet DIU's specific requirements. Anduril's solution will rely on the "Dive-LD" family (Figure 1) of AUVs, which are AI-enabled and capable of performing a range of military and commercial missions. Anduril markets the system as having a "flexible and unique architecture capable of rapid integration of complex payloads and multi-sensor suites" and as being well-suited for undersea battlespace intelligence, surveillance, and reconnaissance; mine counter-warfare, anti-submarine warfare, seafloor mapping, among other mission sets. The system also uses Anduril's AI-driven Lattice platform for mission planning and execution and command and control. In addition to its multi-payload / multi-mission flexibility, the company also highlights the advanced manufacturing processes used in the Dive-LD platform's production, which make it, in the words of the company's chief strategy officer Chris Brose, "quick to produce, economical to manufacture and service, simple to customize, and robust in operation." The AUV announcement came only approximately two weeks after reports emerged that Anduril had been selected along with Boeing, Lockheed Martin, Northrop Grumman, and General Atomics to build an uncrewed Collaborative Combat Aircraft (CCA) that will fly alongside U.S. fighter jets. The company established itself in the U.S. and allied defence industry initially as a software company but has over the last two years acquired companies that have allowed them to build not only the AI-enabled command and control and situational awareness solutions such as Lattice but also the hardware on which these systems will be placed. Notably, the company acquired Dive—maker of the Dive-LD family referenced above—in February 2022 and then UAS maker Blue Force Technologies in September 2023. Blue Force's Fury UAS is likely to be the basis for Anduril's CCA offering. This development of software companies entering the hardware market is not unique to Anduril, nor is it a one-way merging of hardware and software providers. Original equipment manufacturers and defence primes have also sought to capture more of the value chain of their products' lifecycle through the acquisition of software and autonomy startups and through strategic partnerships such as the one between BAE Systems and Obrizum referenced above.

Figure 1: Anduril's Dive-LD AUV platform. Source: Anduril website

2.3	**Evolution, not revolution: Think tank report assesses the impact of the use of drones in Ukraine** Among the report's key findings is that "drones have transformed the battlefield in the war in Ukraine, but in an evolutionary rather than revolutionary fashion" and that "their impact falls short of the truly disruptive change that constitutes a so-called revolution in military affairs" (source) *Assessment:* On 8 February, the Center for a New American Security (CNAS) released a report entitled "Evolution, not Revolution: Drone Warfare in Russia's 2022 Invasion of Ukraine." The report tracked and assessed developments in the drone war between Ukraine and Russia. The main thesis was that while there had been an impressive number of tactical innovations involving drones in Ukraine, the use of drones in the conflict did not constitute a "revolution in military affairs." According to author Stacie Pettyjohn, one important area in which innovation has been short of revolutionary is in the use of autonomous systems. While both sides have attempted to develop and use autonomous systems, "for the most part, Russian and Ukrainian drones remain piloted by humans, are not broadly networked together, and are small, which means their effects tend to be localized." The report also portrays an interesting and iterative contest in which Ukrainian forces have proven consistently more agile and innovative in the use of commercial drones but also one in which Russia has been quick to adapt and even emulate Ukrainian innovations in software and commercial technologies. Moreover, Russia has demonstrated advantage in the development and use of military drones, "which enables its forces to see and strike farther behind the front lines, while Ukrainian forces have gaps in this area." Other selected findings highlighting the use cases, value, and limitations of drones in the Ukraine war include: • The accessibility and affordability of drones is creating new capabilities at a scale that previously did not exist and transforming the battlefield • Surveillance and targeting missions remain more important than drone strikes • Even large numbers of small drones cannot match the potency of artillery fire • Drones do not have to be survivable if they are cheap and plentiful because one can have resiliency through reconstitution • Commercial drones are making it more difficult to concentrate forces, achieve surprise, and conduct offensive operations

2.4	**Estonian group starts work on EUROGUARD USV development program** Baltic Workboats is coordinating the four-year European Union funded program that includes a total of 23 defence companies and research institutes from 10 other EU member states (source and source) *Assessment:* In January, Baltic Workboats kicked-off support to the EURopean Goal based mUlti mission Autonomous naval Reference platform Development program (EUROGUARD). The Estonian company is leading a consortium that involves organizations from Poland, Netherlands, Belgium, Italy, Norway, France, Spain, Denmark, and Sweden. The program is designed to build a vessel capable of several different autonomous operations in coastal areas and is envisioned as contributing "to the need for more rapid response capabilities by well-coordinated EU naval vessel fleets." It will also "enable EU navies to further explore the feasibility to use medium sized semi-autonomous vessels either working independently or as part of a fleet." The European Defence Fund has allotted €65 million to the program, which will cover a large portion of the €95 million total cost. Specific prototype capabilities will be determined through multi-year research and development activities, though autonomous navigation, obstacle and threat detection, and collision avoidance are priorities. Moreover, the EUROGUARD prototype will be modular, allowing it to be assembled based on specific mission needs. Francisco Casalduero, programme manager at the European Commission's Directorate General for Defence Industry and Space said that the program is "a major step forward in EU cross-border cooperation at both industrial and governmental levels in the naval sector" and that it "fosters greater and concrete defence cooperation while providing EU navies with a multipurpose and cost-effective capability for littoral operational environments.

3. Sensors

3.1	**Scaling drone detection technologies is critical to survival in Ukraine** Russian drone use is placing pressure on Ukrainian forces to scale production of technologies designed to help detect targeting and armed drones in order to survive on the current battlefield (source) *Assessment:* The counter-drone fight for Ukraine begins with detection of drones at distance. Whether it is a targeting drone or a loitering munition / kamikaze drone, once Russian drones spot Ukrainian forces there is only a small window of time in which Ukrainian forces can take steps to safely relocate and engage targeting drones. As a result, a small, but important, ecosystem of companies has emerged in Ukraine dedicated to building low-budget drone detectors that use various approaches to detect specific types of drones used by the Russian military, including the Orlan-10 drone used for targeting for artillery and DJI-brand commercial drones. These systems are small—some are handheld—and inexpensive, costing between $100 and $400 per copy. However, as effective as these systems have been to date, the companies producing them have not been able to scale production to keep up with the growing demand. Ivan (*Defense One* uses only first names of interviewees to protect their identities), founder of drone detection company Kara Dag (Figure 2) explained that "there's four, maybe three, maybe four manufacturers of these devices. And I do not know any of them where you can actually purchase it, because they're sold out." Moreover, the supply chain for these innovative products has proven vulnerable to disruption. One option for scaling is for these firms to seek out investment from private capital. There has been some interest from Western private capital firms have started to invest in Ukrainian technology-driven defence startups, even if there remain concerns and constraints in investing in technology that many times is being developed on the fly in an active war zone. In addition, some Ukrainian companies have applied for grants from the Ukrainian government, such as through Brave1, a Ukrainian government defence technology office set up to fund rapid development of innovative defence technologies.

Detection capabilities of the Obriy 1.3 model

Model	Possibility of detection	Frequency bands at which the device can detect a drone It shows at which bands drones are transmitting signals and our ability to detect them. If we can detect signals at all of the bands of a particular drone, the drone can't hide. If, in contrast, a drone has bands where we are blind, the drone can go unnoticed when operating in those bands.				
Quadcopters:		1.2G	2.4G	5.2G	5.6G	5.8G
Dji Mavic 3, Dji Mavic 3 Pro, Dji Mavic 3 Classic, Dji Mavic 2, Dji Mavic 2 Enterprise Series, Dji Mavic 2 Pro, Dji Mini 3, Dji Mini 3 Pro, Dji Mini 2, Dji Air 2s, Dji Matrice 30 Series, Dji Matrice 300 RTK	✅		✅			✅
Dji Mavic 3 Enterprise, Dji Mini 4 Pro, Dji Air 3, Dji Matrice 350 RTK	50/50		✅	⛔		✅
EVO II, EVO II Pro V2, EVO II Dual 640T V3, EVO II RTK Series V3, EVO II Enterprise V2	✅		✅			✅
EVO Lite Series, EVO Nano Series	50/50		✅	⛔		✅
EVO II Pro V3, EVO II Enterprise V3, EVO II Dual 640T V2, EVO II RTK Series V2	50/50		✅		❓*	✅
EVO Max Series	50/50		✅	⛔	❓*	✅
Large russian UAVs:						
Orlan, Zala, Lancet	⛔					
FPVs, classified by their video transmitter type:						
Video at 5.8, telemetry at any frequency	✅					✅
Video at 2.4, telemetry at any frequency	✅		✅			
Video at 1.2, telemetry at any frequency	✅	✅				
Video at any other frequency	⛔					
HDZero Race V2 VTX, HDZero Whoop Lite, Rush Tank Ultimate Plus, TBS Unify Pro32 HV, TBS Unify Pro32 HV, Rush Tank MAX SOLO (2.5W) / SOLO (1.6W), Eachine TX805, Happymodel ELRS Fyujon AIO Board, TBS Unify Pro32 Nano, SpeedyBee TX800 VT, iFlight Blitz Whoop, JHEMCU 2,5 Вт VTX, Diatone Mamba VTX Ultra	✅					✅
Matek VTX-1G3SE Video Transmitter	✅	✅				

** 5600 - 5750 frequencies are available only for Japan; we detect drones on the band from 5650 and above, and do not detect on the band 5600 - 5650*

Figure 2: A screenshot of a description of the detection capabilities of the Obrly 1.3 model drone detector made by Ukrainian company Kara Dag. Source: [Kara Dag website product page]

4. New Weapons

4.1	**DragonFire flies forward: UK developed laser clears key milestone** During trials at the UK Ministry of Defence's (MoD) Hebrides range, the DragonFire directed energy weapon took a significant step forward by engaging aerial targets. The success pushes the joint MoD and industry sponsored program closer to transitioning from research to operational use. Achieving this transition at scale has been a challenge for advanced militaries (source and source) *Assessment*: In January, the UK MoD announced that the DragonFire laser directed energy weapon (LDEW) system achieved the UK's first high-power firing of a laser weapon against aerial targets. Nick Joad of the MoD's Defence Science and Technology Laboratory commented after the test that the "DragonFire uses cutting-edge science and technology and delivers much greater performance than other systems of a similar class. DragonFire provides a step—change in our ability to deal with high-performance and low-cost threats." Both the British Army and Royal Navy are considering using this technology to support layered air defence capabilities. As with all directed energy systems, the DragonFire offers a low-cost alternative for meeting the expanding range of air and missile threats. Rather than having to fire expensive kinetic interceptors against low-cost drones, the UK hopes the LDEW will offer a more affordable option to layered air and missile defence efforts. The next stage in the DragonFire program is to begin the transition from the research phase to operational use. As much value and flexibility as lasers can provide, it is also worth noting that they are not a "silver bullet" for air and missile defence. For lasers to intercept threats they must remain on target for several seconds, meaning that they can only engage one threat at a time. Another form of directed energy weapon, high-powered microwaves (HPMs), are able to more effectively engage swarms or stacks of drones, though these weapons are not as a mature state of adoption as laser weapons. And this leap from science and research and development to operational use at scale has proved a challenge that is now revealing real-world operational risks. Only three days after the MoD DragonFire announcement, *Defense News* published a feature on the increasing frustration of many stakeholders in the United States defence community that directed energy weapons have not been adopted widely enough across the fleet to contribute to U.S. Navy's on-going maritime protection operation in the Red Sea. Vice Admiral Brendan McClane told reporters in January that when he was deployed to the Middle East a decade ago, "the afloat staging base *USS Ponce* had a laser on it. We're 10 years down the road, and we still don't' have something we can field?" The frustration is heightened because the U.S. Navy's efforts to protect global shipping in the region could benefit considerably from the low-cost, deep-magazine capabilities provided by high-energy lasers and high-powered microwaves. They could help conserve high-cost interceptors to be used against more sophisticated threats rather than using them against relatively low-cost Iranian drones. While some U.S. ships do carry directed energy lasers, the weapons have not been deployed at scale and are not being leveraged in the current operation.

4.2	**Chinese scientists resurrect the "dream shell"** The idea for a fast, manoeuvrable shell launched from an electro-magnetic rail gun was originally introduced by the U.S. Navy in 2012 before being abandoned (source—firewalled, accessible source) *Assessment:* Chinese scientists claim to have created a smart shell for electromagnetic rail guns that can travel at a speed of Mach 7 while still receiving navigation signals from China's BeiDou global navigation satellite system, allowing it to "continually adjust its flight path." The scientists maintain that the shell has an error of less than 15 meters, which is, of course, a significant circular error probability if it is aimed at smaller targets. However, as the *South China Morning Post* points out, if it is aimed at a large warship or port, the challenges with precision could be mitigated. The U.S. Navy did pursue a similar program beginning in 2012 but saw no known returns before cancelling its interest in electromagnetic rail guns by 2021. The engineering challenges around developing a weapon that can be launched from an electromagnetic rail gun and still receive signals from a GNSS is significant. Launches from an electromagnetic rail gun create tremendous heat and an intense electromagnetic field that can affect on-board electronics, including electronics required to receive navigation signals. Chinese scientists claim to have devised a work-around for this problem that includes a novel antenna design capable of resisting electromagnetic radiation while still receiving high-precision positioning signals. The plusses and minuses of electromagnetic weapons, especially those placed aboard naval vessels, have been debated over the last decade-plus. As mentioned, the U.S. Navy abandoned its electromagnetic railgun effort believing that the value provided was less than the design and retrofitting challenges of refitting surface fleet vessels with large rail guns and the physics challenges of supplying energy to and sustaining these weapons. Nonetheless, advocates of rail guns do stress their operational advantages in terms of speed, range, and overall cost of the munitions launched from rail guns in comparison to missiles.

4.3	**Taiwan has developed a counter-drone capability** Taiwan's armed forces have reported integrating a new counter-drone weapon known as SKYNET ADS, which was developed by Taiwanese company DronesVision (source) *Assessment:* The hand-held weapon was developed and built entirely in Taiwan and uses a double-barrel design. According to a video placed on the DronesVision website (Figure 3), the system can jam video and GNSS (for example, GPS or BeiDou) signals and even take control of a small drone, forcing it to land. It weighs 4 kilograms, has a range of 2 kilometres, and utilizes three channels to operate. The SKYNET ADS system is part of a broader Taiwanese government effort to build a more robust drone defence capability across the country, including on its remote islands, both in response to China's military build-up as well as to the increase in cross-strait "grey zone" activities, some involving the use of small drones. Most notably, in August of 2022, a Chinese commercial drone captured footage of Taiwanese soldiers on Erdan islet throwing rocks at the drones (Figure 4). The video later went viral in China, leading to ridicule of Taiwan's military on Chinese social media. Per a video report published on Hindustan Times YouTube channel, Taiwan's Kinmen defence command—Kinmen is a province consisting of islands that are only a handful of miles away from the city of Xiamen in China's Fujian province—confirmed the event took place and asserted that the footage is "another example of China's cognitive warfare against Taiwan and an attempt to denigrate its armed forces." The 2022 event served as a catalyst for Taiwan to improve its drone defences both in Kinmen and throughout the country.

Figure 3: A screenshot from a promotional video on DronesVision's website that shows the SKYNET ADS system being used. Source: DronesVision SKYNET ADS product page

Figure 4: A screenshot of the August 2022 incident in which a Chinese commercial drone captured images of Taiwanese soldiers throwing rocks at it. An incoming rock is visible in the bottom centre of the screen shot while two Taiwanese soldiers are visible in front of and to the left of the military building. Source: Taiwanese News YouTube channel.

5. Digital Communications

5.1	**Fake news, deepfakes, and the future of disinformation** The reporting period saw multiple examples of how synthetic media and disinformation were spreading relatively unchecked with actual and potential implications for defence and security communities as well as for democratic states and societies (source and source) *Assessment:* On 3 February, *AFP* published a "fact check" report addressing a YouTube video that purported to show a Philippine naval vessel shooting down a Chinese surveillance drone in Philippine territorial waters that are also claimed by China. The video, which was posted on 19 December 2023, is titled "BRP Antonio Luna has shown its might." (Figure 5) It was released during heightened tensions between the Philippines and China as China aggressively pressed territorial claims to features and islands that are within territorial waters belonging to the Philippines. While the video has developed a reasonable amount of traction—27,000 views by early February—the events depicted in it never happened. Indeed, the video includes language saying it is for entertainment purposes only. The spread of the video eventually led to the Philippine Navy having to address the issue, releasing a statement saying that "no such shooting of a drone happened." The images in question were from March 2020 and depicted a drone being shot down over Syria. This instance of disinformation ultimately did not lead to an appreciable increase in tensions between Philippines and China or create domestic pressures in either country to escalate the already sensitive situation in the South China Sea. Still, it is easy to see how such fake videos can amplify real world anxieties by playing into growing nationalist sentiment across the region or creating inaccurate perceptions among key military and political decision-makers in a time of crisis. This is especially the case as the technology around synthetic media (i.e., deep video and audio fakes) improves and as more actors view even lower quality deepfakes as an easy way to create confusion and doubt among targeted constituencies. For example, in January, a synthetic audio deepfake of U.S. President Joe Biden was sent to thousands of 2024 Presidential primary election voters in New Hampshire. The recording encouraged Democratic voters not to vote in New Hampshire's primary and was spoofed (or altered) to appear as if it came from the head of the New Hampshire Democratic Party. Again, the proximate damage caused was minimal—President Biden is the presumptive nominee in New Hampshire and across the country—but that lack of immediate impact should not dampen concern over how deepfakes can shape narratives and further undermine the concept of shared truth. Robert Weisman, president of the U.S.-based political advocacy group Public Citizen, summed up the broader challenge revealed by the recent proliferation of deepfakes and disinformation: "The New Hampshire deepfake is a reminder of the many ways that deepfakes can sow confusion and perpetrate fraud."

Figure 5: A screenshot from the YouTube video incorrectly depicting the downing of a Chinese drone over the South China Sea in December 2023. Source: AFP Fact Check

5.2	**Now you see me, now you don't: U.S. Marines hide command posts through digital manipulation** The exercise reveals low-cost, clever ways to hide electronic signatures of increasingly vulnerable command posts (source) *Assessment:* U.S. Marines deploying to the Indo-Pacific theatre for exercises at the end of 2023 have developed means of hiding their command posts using local cell phone networks and other commercial technologies. Militaries both large and small have become concerned about the viability of modern, static command posts in an operational environment in which there are near constant efforts to detect electromagnetic signatures that could represent a fixed military position. In this environment, radio emissions could give away the position of a command post. However, when Marines were able to connect through host-nation Wi-Fi, they were able to hide their signature while still carrying out most operational tasks. Using local Wi-Fi allowed the Marines to blend "right into the environment" from a signature management perspective. The ability to manage the signature of command posts is part of a broader effort to make them more survivable on the modern battlefield. Army Chief of Staff General Rangy George noted at the Association of the United States Army conference in October 2023 that if the U.S. Army "[slogs] around the battlefield with massive operations centres, which are difficult to set up and often contractor-supported, we will get pounded."

6. Cyber

6.1	**South Korea and Germany release joint warning of North Korea cyber-theft of defence technology** Activities referenced in the report took advantage of social engineering and indirect attacks to access sensitive information from defence companies over the last several years (source and source) *Assessment:* On 19 February, South Korea and Germany released a joint cybersecurity advisory warning that North Korea is using cyber espionage to obtain military technologies and advance its weapons programs. The advisory was released by South Korea's National Intelligence Service (NIS) and Germany's Federal Office for the Protection of the Constitution (BfV). According to the NIS, "both organizations believe that North Korea has placed strengthening its military power as a priority for its regime, is focusing on stealing cutting-edge defence technology from around the world and is using the stolen technology to develop strategic weapons such as reconnaissance satellites and submarines." The organizations highlighted a specific attack against a maritime shipping and technology research centre in late 2022 (Figure 6). The attack initially infiltrated a supplier for the research centre's servers before subsequently compromising the research centre itself. Loose security protocols related to remote server maintenance were cited as one vulnerability with the German version of the advisory stressing that the North Korean actor took advantage of a "trustful relationship" between the research centre and its maintenance services supplier to facilitate the attack. The NIS and BfV also highlighted the social engineering efforts of Lazarus Group, a suspected North Korean-backed hacking organisation. As part of the group's "Operation Dream Job", Lazarus Group has set up fake profiles on LinkedIn to pose as recruiters on LinkedIn or other job portals. The hackers target individuals in roles at defence companies that provide access to internal systems and work to build trust with them, eventually sending files with malware to gain access to the company's network.

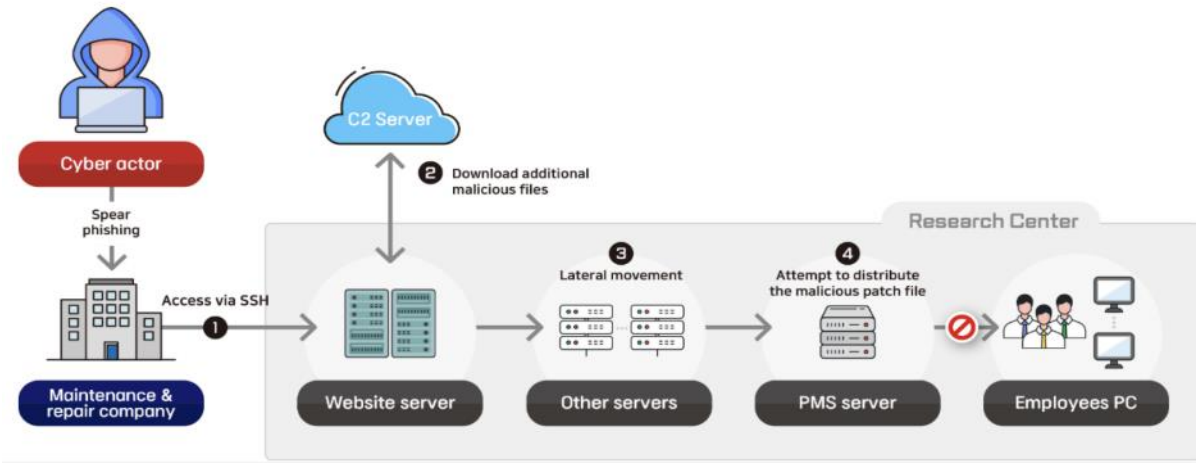

Figure 6: The attack flow of a 2022 intrusion campaign against a maritime and shipping technology research centre. Source: German Federal Office of the Protection of the Constitution

7. Space

7.1	**India sharpening its focus on space capabilities, partnerships** In comments during the DefSat Conference and Expo held in New Delhi in early February, the Indian chief of defence staff General Anil Chauhan articulated several priorities for the military's space-based capabilities including deepening collaboration with civil and commercial space entities and leveraging international partnerships *Assessment:* General Chauhan stressed the need for "an integrated approach with the civil space sector as [the Indian military's] partner. He also provided a list of priorities for continued development that included: increased launch capacity, including on-demand launch, and improved capabilities in nanosatellites, hyperspectral imaging sensors, satellite antenna arrays, reusable rockets, and advanced propulsion. According to *Shephard Media,* the comments were made in a broader context in which many in India perceive the country is falling behind China in the establishment of a comprehensive space-based intelligence, surveillance, and reconnaissance capability and that the military has previously moved too slow to establish a military space command and create the necessary space-based capabilities. One area in which India has seen progress in recent years is in the establishment of partnerships with other nations to share industrial capacity and technology, including the signing of a MoU between New Space India and Arianespace for satellite launches. India's SatCom Industry Association also signed an MoU with the Space Industry Association of Australia during the February conference. While India has long espoused the importance of increasing independence in its domestic defence industrial base, these relationships are seen as an important step in augmenting current capabilities and progressing toward more technological independence in space capabilities.


https://deftech.ch/