Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

DEFTECH-SCAN

February 2026

OTH INTELLIGENCE GROUP

deftech.ch/scans

Dear Reader,

Welcome to this edition of Deftech-Scan highlighting a defence landscape defined less by grand breakthroughs than by steady, pragmatic acceleration.

Across this issue, several clear clusters emerge. **First, AI is no longer a futuristic talking point but an operational reality**, shaping command systems in Russia, accelerating North Korean cyber capabilities, enhancing aircraft maintenance, and quietly embedding itself in procurement networks and cognitive warfare. If software is eating the world, it appears the battlefield is next on the menu.

Second, autonomy is scaling. From drone swarms edging closer to operational deployment, to uncrewed surface vessels searching for their place in fleet architecture, to export-ready anti-submarine drones, robotics is moving from experimentation to integration, albeit not always at the speed industry might prefer.

Third, adaptation is everywhere. Sanctions breed crypto workarounds. Logistics challenges spur additive manufacturing. Militaries rethink humans as "weapon systems" to be sustained as carefully as hardware. Even cargo ships are having existential upgrades.

The pattern is consistent: **iterate quickly, deploy practically, adjust constantly**. Not always elegant, but undeniably effective.

We hope you find it both useful and thought-provoking.

Foresightly Yours,

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

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

1. Applications of AI and data

1.1	**Russia is reshaping its command and control for AI-enabled warfare** A Center for Strategic and International Studies (CSIS) study assessed how Russia is adapting its command and control (C2) architecture under wartime pressure and how these changes shape the country's incremental move toward battlefield-required software solutions. (source) *Assessment:* The February report outlines seven key findings about Russia's C2 transformation and use of AI on the battlefield in Ukraine. Together these findings reflect the report's main theme that "Russia is not chasing technological elegance or conceptual completeness but rather applying AI selectively and ruthlessly in service of battlefield effectiveness." 1. Russia is no longer prioritising the construction of a single, comprehensive automated C2 structure comparable to Western joint concepts; instead; it is reallocating effort toward tactical, task specific software, driven by battlefield necessity 2. Because uncrewed systems now conduct up to 80 percent of Russian fire missions, the centre of gravity in C2 innovation has shifted toward software that manages drones and integrates them with artillery and other fire units 3. The Russian military assesses its AI capabilities for visual and audio data processing as relatively mature, placing computer vision, sensor fusion, and signal analysis at technology readiness level (TRL) 6-9, while natural-language processing remains at an early, experimental stage, TRL 1-3. 4. Within Russian C2 systems, AI is primarily envisioned as a support function rather than a replacement for human decision making 5. Russia began its C2 digitalisation effort by building a dense layer of standards governing terminology, system architecture, hardware-software integration and information management 6. To enable AI-driven tactical software, the Russian military launched a systematic data collection effort in 2025 focused on uncrewed operations and strike outcomes 7. Despite efforts to reduce dependence on foreign commercial technologies, Russia's military AI development remains heavily reliant on open-weight models and civilian software ecosystems. The CSIS analysis is based on open-source research, mostly comprising Russian primary materials as well as Russian Telegram channels and closed or semi-closed groups associated with civilian engineers, volunteer technologists, and military-affiliated developers supporting the Russian war effort.

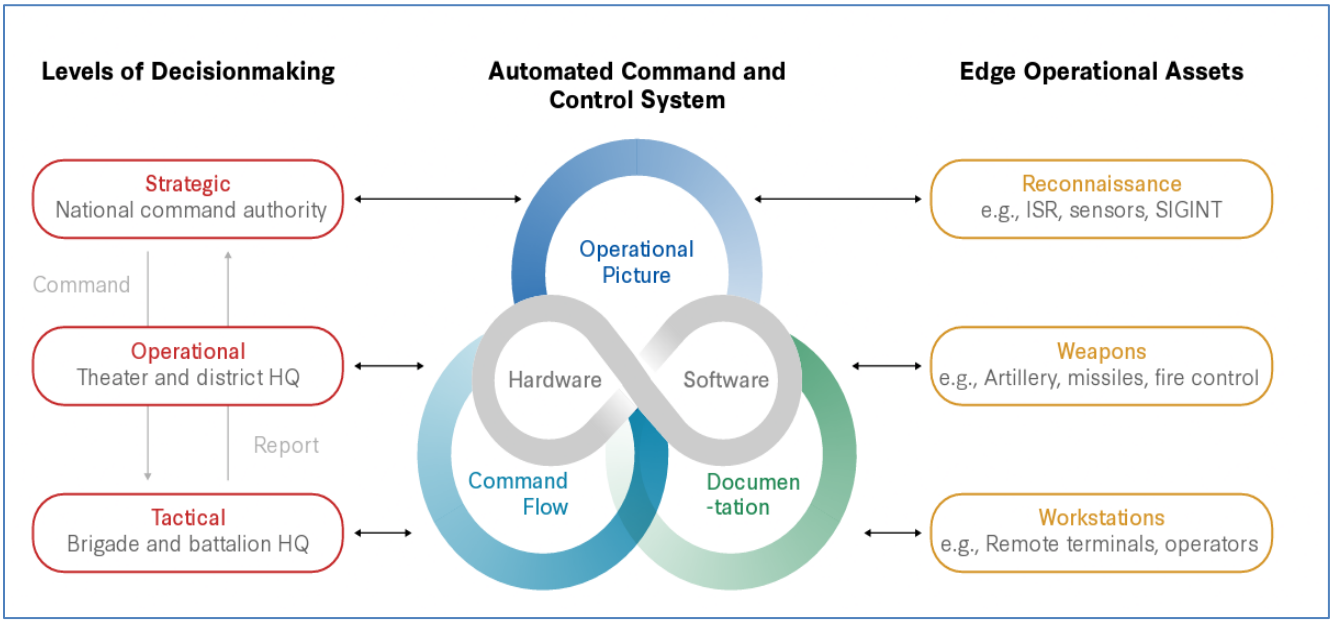

Figure 1: A CSIS figure depicting an Automated Command and Control System (ACCS) Architecture, described as a "system of systems in which command structures, operational headquarters, reconnaissance assets, and weapons platforms are interconnected within a single integrated environment for decision making and execution." Source: CSIS

1.2	**North Korea has developed AI capabilities ready for military use** A report from the South Korean Institute for National Security Strategy (INSS) assesses that North Korea AI capabilities have matured to the point where they can be used in military and cyber operations. These capabilities could support surveillance, target identification, voice impersonation, and cryptocurrency theft. (source and original source) *Assessment:* The report was based on analysis of several 2025 studies from North Korean scientific and academic institutions that suggest progress in the development of military and security-focused applications of AI. For example, one report revealed an improved facial recognition system, which can reportedly identify faces even in low-light or low-resolution footage. Another study documented multi-person tracking algorithms demonstrated on sports footage. The INSS authors believe the technology could be utilized in CCTV or drones for real-time automated surveillance of borders, cities and military installations. Of particular concern to the authors were North Korean advances in speech synthesis technology optimized for mobile devices. This technology could facilitate voice impersonation and psychological operations, potentially enabling "immediate voice impersonation in calls and messaging apps." Such a capability could be used for "identity obfuscation, disruptions of command-and-control communications and more effective social engineering operations." The authors also claimed that North Korea is leveraging AI tools to dramatically accelerate cryptocurrency theft operations, asserting that "North Korean actors rely on AI throughout the reconnaissance, social engineering, phishing and money laundering stages…thereby automating, parallelizing and reducing time delays." Collaboration with Russia and China was cited as a key accelerant of North Korea AI deployment.

1.3	**AI-enabled system is making confined space maintenance easier and safer** The US Air Force is deploying the Integrated Respirator Information System (IRIS) to improve the process of maintaining aging aircraft platforms like the KC-135. (source and source (possibly firewalled)) *Assessment:* The process of maintaining refuelling aircraft has not fundamentally changed in several decades. Technicians crawl through tight, dirty spaces, cleaning sealant on fuel tanks and tightening loose rivets by hand. The tanks they operate in are cramped and the maintainers are equipped with "little more than a flashlight, some tools, and shaky comms." According to *Business Insider,* "it can be hard to breathe, the air smells like jet fuel, the fixes aren't always clear, and the punishing work can be dangerous if done wrong." To make this process easier, safer, and more efficient US companies MetroStar and ActionStreamer developed IRIS, which equips maintainers with an AI-enabled, hands-free wearable system that provides real-time video, audio, and lighting. The solution connects directly to a mobile workstation and remote analysts, enabling streamlined inspections, expert support, and future integration with advanced computer vision analytics. AI supports this process by compiling data, handling documentation, and enabling real-time remote expert guidance to increase safety, reduce inspection times, and boost fleet availability. The Air Force is experimenting with IRIS to modernize the maintenance of the KC-135 refueler at RAF Mildenhall in the United Kingdom. The technology rests on top of the face mask tanker maintenance workers wear. It features a high-definition video camera, a two-way communications system that goes inside the mask, and a hands-free light. The system shows everything the technician sees to those outside the fuel tank and allows them to communicate with the team. It also connects to a mobile workstation outside the aircraft, which can host up to four IRIS units simultaneously. The support team can see what the technician sees, talk them through the work, and record the footage. ActionStreamer CEO Bob Lento told *Business Insider*, that there was some concern among maintainers at Mildenhall about the system when it was first deployed, but that the feedback after a week of use was very positive. Overall, MetroStar's website claims that IRIS will make confined-space inspections 60 percent faster, reduce maintenance time by 35,000, and add 7,000 days of aircraft availability over the course of a year.

2. Robotics and Autonomous Systems

2.1	**Renault joins the fight** French carmaker Renault announced it will start manufacturing long-range strike drones under a contract with the country's Directorate General for Armament that is worth as much as €1 billion over 10 years. Renault will work in partnership with local defence contractor Turgis Gaillard. (source and source) *Assessment:* The company has confirmed that it will build up to 600 long-range remotely guided munitions per month at its factories in Le Mans and Cleon, west of Paris. The drones are expected to be like Iran's Shahed drone that can also be used for intelligence gathering and observation. As reporting from *Defense News* notes, "Both Russia and Ukraine are increasingly using such cheap long-range drones for deep strikes and to overwhelm air defences." A statement from Renault highlighted the company's "sought-after expertise in designing, industrialization and mass-producing high-tech objects while controlling quality, costs, and deadlines." French President Emmanuel Macron urged French industry to move to a "war economy" in June of 2022. In January 2026, Macron warned the French defence industry to speed up production, or the government will seek alternative European solutions. In a January 2026 speech, Macron criticized the development of French industry since the President moved industry to a war footing, saying: "a lot of efforts have been made. I acknowledged it; we have doubled, sometimes tripled, our production capacities and rates. Let's be honest with ourselves. Are we truly operating under a war economy? The answer is no. Because if we were at war, I would like to think we would not be producing as we are now,"

2.2	**Almost there? French Army and Thales suggest autonomous drone swarms are only two years away** Eric Lenseigne, vice president for drone warfare with Thales, asserted that real use cases for autonomous drone swarms will be deployed in certain units "within two years" in remarks made at the Forum Innovation Défense in Paris in December. (source) *Assessment:* While swarms of drones have been deployed in Ukraine, these systems are controlled remotely by a large number of dedicated operators. The future of drone swarming is in the deployment of large number of autonomous systems that can sense, decide, and act collectively with limited human intervention or control. Lenseigne said that Thales experiments on drone swarms "show that we are on the verge of" having systems that will allow for true implementation of autonomous swarms and that all the building blocks for swarm technology already exist. Swarms are viewed as an important capability in countering the increasingly capable anti-access/area denial systems by saturating and outpacing air and missile defence systems. They can also carry a range of payloads—kinetic, electronic, surveillance—that can work together to defeat these systems. Another use case for swarms is to resupply troops stuck in combat positions in environments in which movement along the front lines will be detected and targeted quickly. Previous DEFTECH Scans have highlighted the impact continual drone surveillance at the front lines have had on military medicine, forcing front line medics to carry out more medical treatment due to the risk of moving wounded soldiers to rear-guard medical stations. Using drones to bring in additional medical supplies could be a life-saving swarm application. One interesting aspect of employing swarms is the psychological impact they might have on human operators who will soon be confronted with a dehumanized battlefield that includes swarms of robots that move faster and respond to a changing environment faster than humans can track. While challenges remain for developing and deploying autonomous drone swarms—for example, resolving ethical issues, hardware integration, power sources--Lenseigne argues that "within two years, we'll indeed have real use cases deployed in certain units, and widespread adoption will quickly follow, because the benefits of swarms will be quite obvious."

2.3	**Challenges scaling the USV market** Many companies are engaging the US Navy to respond to nascent demand for uncrewed surface vehicles (USVs), And while these systems are conceptually crucial to the future of the Navy's force structure, progress for these companies have been slow as the Navy works to develop more detail about how and at what scale they will be incorporated into the future force. (source) Assessment: Adoption at scale of emerging technologies and the capabilities they enable can be undermined by a range of factors that go beyond technological development. For example, militaries may have an acute appreciation of the value new capabilities can bring but lack a clear understanding of how best to use these systems, train operators on how to use them, or understand how to incorporate them into legacy force structures. Reporting from *Defense One* indicates that this may be the case with US Navy efforts to adopt USVs. Experiments with USVs are continuing under at least three Navy commands, and senior leadership is developing plans to buy, operate, and maintain USVs as they seek to achieve affordable scale and meet the threats of the modern maritime environment. However, concern is growing within the burgeoning industry seeking to meet this demand that the Navy can scale development and adoption of USVs in the short term, creating challenges for the "several dozen" companies current developing USV solutions in anticipation of future Navy demand. Rylan Hamilton, CEO of Blue Water Autonomy, which is developing a 190-foot robot patrol craft, said that no one "questions whether [USVs] have a place in the fleet architecture. It's really: 'How long is it going to take to get some of these vessels out into the fleet and operating, so the end user of the fleet can really figure out how they want to use them and how many they actually want.'" Absent an enhanced plan and structure for integrating these capabilities, USVs "could stack up in storage because the service's operations, training, and sustainment models haven't been tweaked to match." The Navy envisions a prominent role for medium and large-sized USVs, but to date has largely focused on small drone boats, a market that "is accelerating a lot quicker" than the market for larger USVs. And a possible promising development for industry is that the Navy is expected to announce the Modular Attack Surface Craft (MASC) program. The smallest version of MASC is expected to carry a 20-foot payload, while the largest could carry four 40-foot containers. Hamilton believes that the program "has been a really strong signal to industry."

2.4	**China's "X-port" strategy for anti-submarine warfare drone** Chinese state-owned enterprise Aviation Industry Corporation of China (AVIC) has displayed its Wing Loong-X (WL-X) variant uncrewed aerial system (UAS) at several defence exhibitions in emerging markets. The WL-X is reportedly the world's first anti-submarine warfare (ASW) capable UAS and appears to have been designed to take advantage of growing demand for advanced capabilities in emerging markets. (source, source, source) *Assessment:* A full-scale model of the WL-X was first seen outside of China at the Dubai Air Show in November. It has subsequently been displayed at the World Defence Show in Saudi Arabia and the Singapore Air Show, both held in February. The long-range, medium-altitude, heavy-load UAS was developed specifically for the ASW mission. It is designed to deploy sonar buoys, conduct acoustic analysis, coordinate with other airborne or naval platforms in real-time, and launch advanced anti-submarine torpedoes. Perhaps most importantly, the aircraft has an extended endurance of up to 40 hours, considerably more than even the most advanced Western crewed ASW and maritime surveillance assets, such as the P-8 Poseidon, which has a max flight time of approximately 10 hours. The ASW mission is gaining in importance globally, due to the proliferation of submarines, increased development of uncrewed underwater vehicles, and growing concern over the vulnerability of undersea cables. It appears the system was designed primarily to take advantage of the successful export of previous Wing Loong variants and growing demand for more advanced uncrewed systems in emerging markets that cannot gain access to Western military equipment. Frederico Borsari, a resident fellow with the Center for European Policy Analysis noted to *Defence News* that efforts to export this system are likely to find traction, especially among "countries that cannot access or afford Western due to cost, export controls, or political constraints." Saudi Arabia, the UAE, Egypt, Pakistan, Morocco, Algeria, Indonesia, and Nigeria are among the growing list of countries operating other Wing Loong models.

Figure 2: The Wing Loong-X on display in Saudi Arabia. Source: South China Morning Post

3. Manufacturing and Industry

3.1	**An additive manufacturing breakthrough?** US Air Force and Marine Corps maintainers used additive manufacturing to print a part to return a US Air Force F-15 Eagle to service within hours, several months ahead of its projected return to service date. (source and source) *Assessment:* After Air Force maintainers at Kadena Air Base in Okinawa discovered the aircraft's right-hand cockpit cooling duct was cracked, they estimated that the aircraft would be grounded for three to four months using traditional repair processes. Navy Air Systems Command Additive Manufacturing Program Manager Theodore Gronda stated that this "was a situation where a multi-million-dollar aircraft was going to be sideline for months due to the lack of a part in the supply system." The Air Force's 18th Maintenance Group (18MXG) originally printed out two prototypes but experienced technical difficulties. They then contacted the Marine Aircraft Logistics Squadron 36 (MALS-36) to leverage its on-site additive manufacturing equipment to help repair the cooling duct. Two prototypes were printed, delivered, and fit checked in less than 12 hours. The Marines also developed an improved design that reduced the part's print team by two hours and "the duct's new printing requirements are now part of the Air Force's [additive manufacturing] technical publications and will be used for similar repairs across the F-15 community", according to Air Force Captain Diego Carrillo, a depot liaison engineer. In addition to the immediate benefits of dramatically reducing the time the F-15 was unavailable, the development reinforces the value that additive manufacturing can deliver in an era in which combat logistics are likely to be highly contested, complicating a challenge for many militaries throughout the world. In fact, contested logistics was included as one of six priority technology areas published by the US Undersecretary of Defense for Research and Engineering (USDR&E) in November 2025 in an effort to "reimagine sustainment in disrupted or denied environments."

Figure 3: A list of the six priority technology areas being pursued by the United States DoD. Source: Undersecretary of Defense for Research and Engineering

3.2	**Crypto adaptation: Russia moving to crypto to fund procurement for key inputs into military equipment** United Kingdom think tank Royal United Services Institute (RUSI) published a report in February detailing how the global crypto economy is feeding Russia's acquisition of Common High Priority Items (CHPI) to get around sanctions. The report reinforces the importance of the global technology supply chain while also reflecting how crypto technologies are being employed at a state level to support military procurement (source) *Assessment:* The report, entitled "The Shadow Crypto Economy Feeding Russia's War Machine", asserts that "crypto is embedded in Russia's procurement model, allowing it an access to CHPIs that international sanctions were intended to deny." CHPIs include microelectronics, navigation equipment, and advanced machine tools essential to produce missiles, drones, and heavy artillery." Sanctions initially did disrupt established supply chains. However, Russia has adapted and has cultivated a complex and adaptive web of transshipment routes and evasion techniques that involve traditional laundering methods. As international banks tightened controls to avoid secondary sanctions exposure, though, Russian importers turned to crypto-enabled payment systems to settle cross-border transactions outside the reach of Western financial regulators. The report singles out Garantex and its successor Grinex as being central nodes in Russia's crypto ecosystem as well as the Exved payment agent and the rouble-backed stablecoin A7A5. Over the counter (OTC) brokers have emerged as a critical and opaque layer in this ecosystem—the report refers to them as "the blindspot." These brokers are responsible for converting rouble funds into procurement-ready stablecoins through informal, trust-based networks that evade standard compliance tools. The publication concludes that sanctions have "had a tangible impact on Russia's procurement environment" and have increased costs, complexity, and risk for Russia's efforts to procure CHPIs. Still, "they have not halted procurement. Instead, they have driven adaptation." The authors argue that addressing this challenge requires a fundamental shift from entity-level designations toward ecosystem-level disruption — integrating trade intelligence with financial enforcement, investing in human intelligence on OTC networks, applying network-based sanctions targeting successor entities and bridging assets, and engaging permissive jurisdictions diplomatically. Without such a coordinated approach, sanctions will continue to reshape procurement routes without cutting off the financial mechanisms that sustain them.

4. Human Protection and Performance

4.1	**Holistic fitness? US Army exploring ways to more effectively create and sustain "human weapon systems"** New approaches to personnel training were discussed at a US Army symposium on human performance held at Fort Benning, Georgia in January. Benning is set to become the headquarters for Army holistic health and fitness training. (source) *Assessment:* At the centre of the discussion was the concept that the military should move away from creating "super athletes" to build and, crucially, maintain the ability to wield the weapons and systems of "an ever-more-robotified" battlefield. Drew Hammond, a human-performance specialist who works with the US Special Operations Command (SOCOM), told attendees at the Human Performance Symposium that "we're moving away from this kind of antiquated idea of very visceral combat experiences." Combat effectiveness now requires developing "a lot of the intrinsic motivators that soldiers may not necessarily have prioritized years ago when we all focused on was [physical training] scores. It's the ability to be cognitively present in what you're doing." A key component of this shift is the increased incorporation of wearable devices that monitor sleep and wellness in addition to other traditional benchmarks to provide a fuller data picture of how soldiers are actually feeling and performing. For example, they will allow leaders to collect "different metabolic markers, inflammation markers" as well as "stress management data." Chris Myers, a researcher at the US Air Force Research Lab (AFRL), believes that a fundamental rethinking of what military activity is necessary in an age dominated by rapid technological innovation cycles and faster, data-fuelled operations. In this environment, it is more appropriate to consider training and sustaining human operators like the military does for a complex weapon. According to Myers, "when you start looking at our human beings as a human weapon system, you can start looking at it through a lens of acquisitions, which really has three different components: procurement, fuelling and sustainment, and disposition. So basic training, feeding and nutrition, and actually monitoring the operator's health and performance—not just yelling at them to do more."

5. Connectivity

5.1	**NATO Chief Scientist releases report on Cognitive Warfare** The report from the NATO Chief Scientist stresses the importance of investing in the ability to understand human cognition and defend against efforts to manipulate public opinion and carry out hybrid attacks and to operate more effectively in an environment in which cognitive capabilities are crucial. (source) *Assessment:* The paper begins with a description of how changes in the strategic environment have led to the re-emergence of Cognitive Warfare as a critical component of conflict. NATO defines Cognitive Warfare as "the fight for Cognitive Superiority" and arguing that "contesting in this environment compromises deliberate, synchronized military and non-military activities throughout the continuum of competition designed to gain, maintain, and protect cognitive advantage." Key aspects of Cognitive Warfare include adversaries influencing cognition and behaviour to gain advantage on multiple levels: • **Societal level**: Democratic rule of law values and social contract • **Group level:** Destabilizing trust and creating polarization • **Individual level**: Attitudes, decision-making, and behaviour Traditional tools used to gain advantage in the cognitive domain include Psychological Operations (PsyOps), Information Operations (InfoOps), and Strategic Communications (STRATCOM). While the report argues that Cognitive Warfare is broader than these three tools, they have been supercharged by the emergence of new modes of communication and technological capabilities, especially AI, that allow for increased scale, precision, and range of message distribution. This makes societies and polities more vulnerable to efforts to "alter human behaviour through cognitive effects using any means, including advanced technologies, without knowing the outcome of the behavioural change." This type of conflict is characterized by adversaries: • Not necessarily targeting specific audiences and objectives • Not being a solely military challenge nor mission-oriented • Often being designed to create chaos and complexity below the threshold of armed conflict • Creating a cognitive battlespace using multiple actions or interference to manipulate adversaries The report also lists seven focus areas of NATO Science & Technology's approach to understand and combat adversary Cognitive Warfare efforts: Situational Awareness/Sense-making; Cognitive Effects; Modus Operandi; Technology Enablers and Force Multipliers; Cognitive Neuroscience; Cognitive and Behavioural Science; Social and Cultural Science, as listed in Figure 5 below.

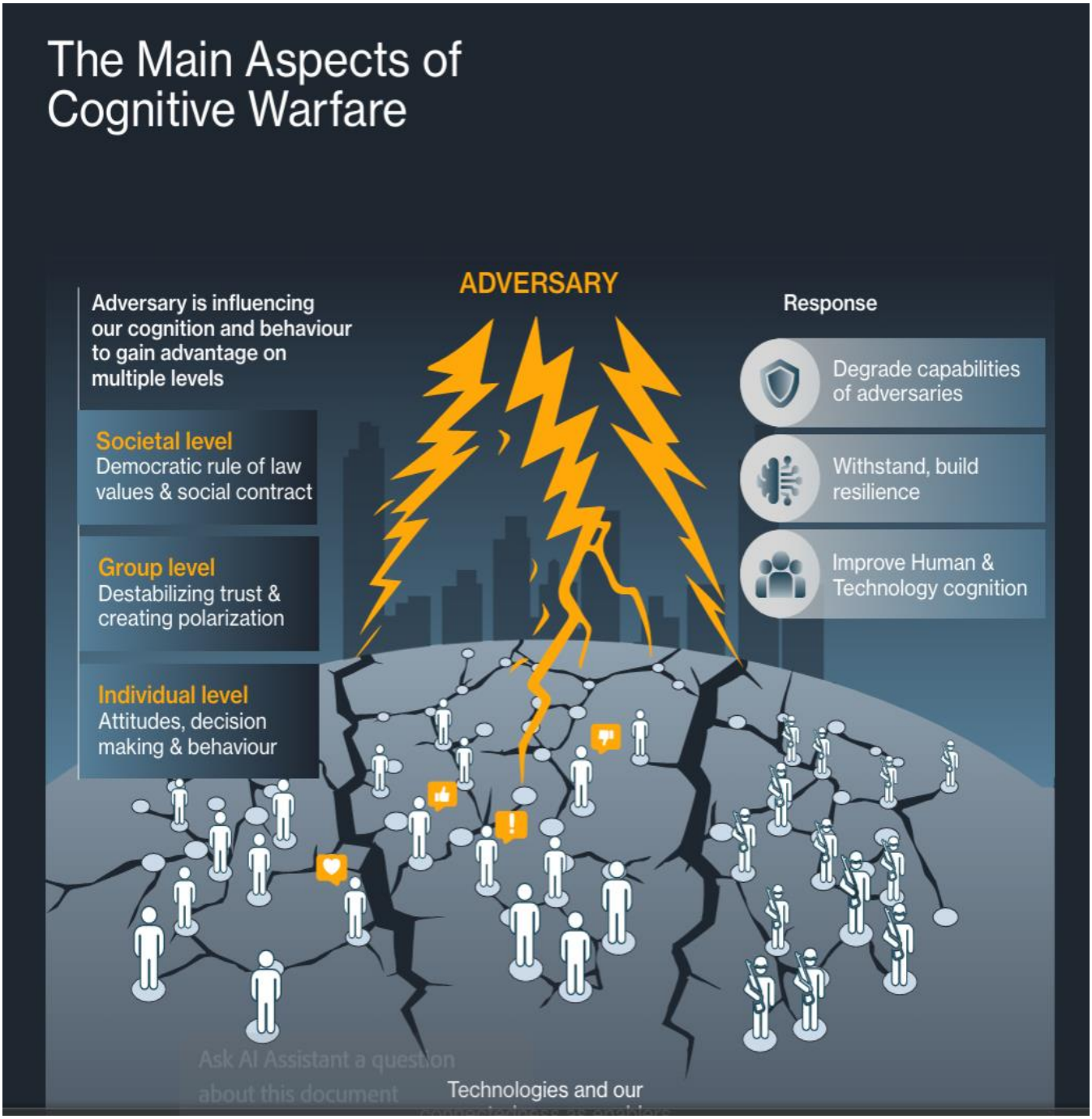

Figure 4: An image depicting the aspects of Cognitive Warfare. The lightning bolts indicate that Cognitive Warfare may target human (military and civilian population) as well as artificial cognition. The left side of the illustration shows effects at individual, group, and societal levels. The connectedness between individuals (connected dots) is increased by modern technologies, facilitating the spread of information, enabling new forms of deception (e.g., deepfakes), and often replacing human cognition. The right part of the figure shows three main responses to Cognitive Warfare: degrading adversaries' capabilities, increasing resilience to withstand attacks, and improving human and technological cognition. Source: Cognitive Warfare, NATO Chief Scientist, illustration by Prof Dr Jose Kerstholt, Organisation for Applied Scientific Research, The Netherlands)

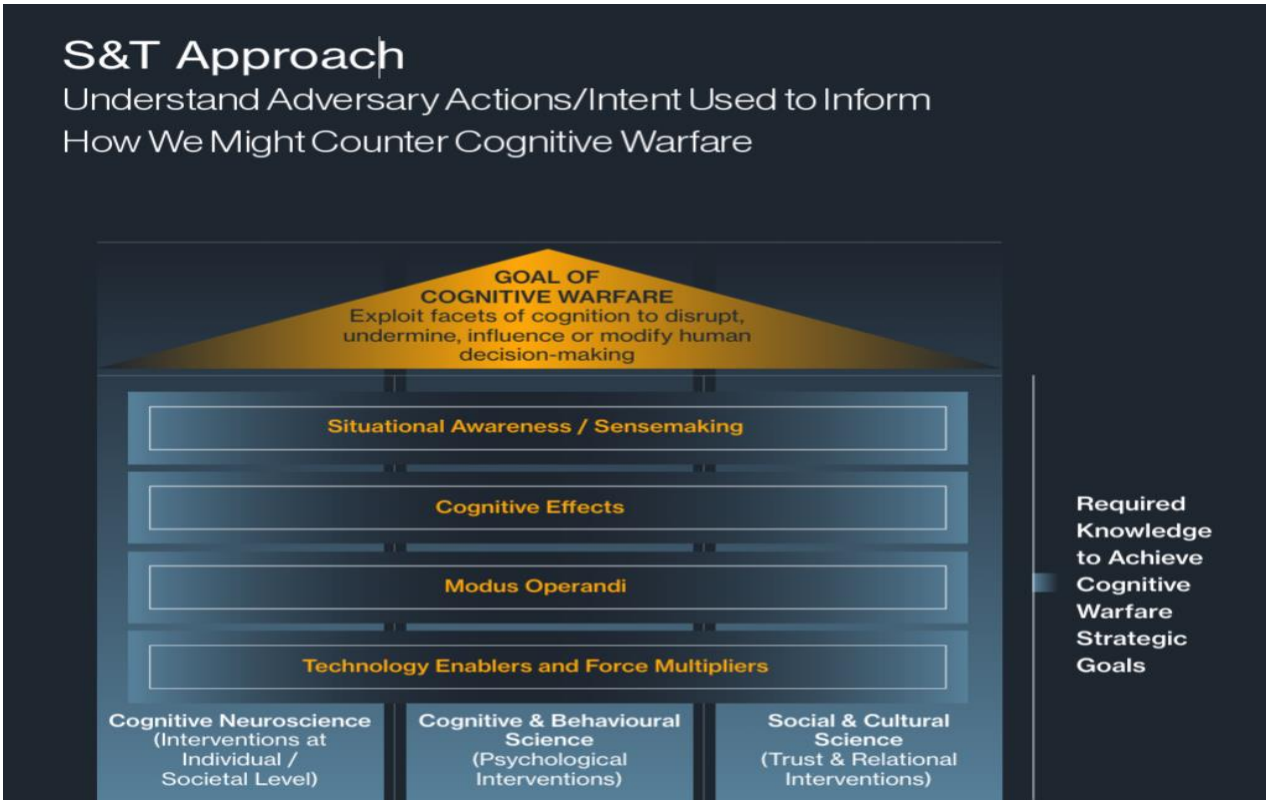

Figure 5: The House Model for countering Cognitive Warfare developed by NATO STO HFM-ST-356. Source: Cognitive Warfare, NATO Chief Scientist

5.2	**All jammed up: US special operators want larger ranges for electronic warfare training** US special warfare trainers are asking government regulators to expand the test ranges for electronic warfare (EW) and drones to better replicate the importance and scale of drone and EW activity on modern battlefield environment (source) *Assessment:* The Ukraine War has emphatically demonstrated how central drones and EW measures such as jamming cellular and GPS signals have become to modern conflict and an ever-more robotic battlefield. As US Special Forces Major General Jason Slider noted in a statement, "never again will there be a time in warfare where a soldier doesn't throw a piece of robotic kit onto the ground, into the water, or into the air to perform some tactical task associated with aiding a partner force, gaining advantage over an adversary, and closing with and killing the enemy." Training for this expansive, crowded, and contested environment is complicated in the United States due to civil regulations about when and where the military can jam signals and fly drones. Representatives from US Army John F. Kennedy Special Warfare Center are seeking to have "uncomfortable discussions" with civilian and federal authorities to get access to more jammable space to train how to operate amid jamming that is far more powerful and ubiquitous than even in the recent past. The US Congress has also engaged in this issue. The most recent version of the National Defense Authorization Act includes provisions to link testing sites to improve range availability and mandates that EW become a feature in certain future exercises involving special operations forces.

5.4	**China rehearsing cyberattacks on neighbours' critical infrastructure** Documents reviewed by Recorded Future News appear to show that China is using a secret training platform to rehearse cyberattacks against the critical infrastructure of its closest neighbours. (source) *Assessment:* The training platform, known as "Expedition Cloud", is built by a company called CyberPeace, "which celebrates extensive links to the country's government and military on its website." The platform allows operators to rehearse cyberattacks against replicas of real network environments belonging to China's neighbors in the South China Sea. It specifically targets critical infrastructure sectors including power, energy transmission, transportation, and smart home systems. The platform is structured around two distinct operational teams: a reconnaissance group that maps the simulated target network and identifies potential access points, and an attack group that uses that intelligence to execute planned operations. Every action taken during exercises is meticulously logged, allowing analysts to reconstruct, replay, and refine attack methods over time. The system features strict operational security and network segmentation, leading experts to conclude it is being used for classified purposes and functioning as a rehearsal environment for real-world offensive operations. Independent cybersecurity experts consulted by Recorded Future News expressed high confidence in the authenticity of the documents, describing the find as extraordinary and unprecedented in the level of detail it provides about China's offensive cyber preparations. China has previously denied conducting offensive cyber operations, but Dakota Cary, a specialist on China for cybersecurity company SentinelOne told Recorded Future that "this was created to meet the needs of a state customer." Perhaps most consequentially, experts highlighted the platform's design reflects increasing automation and AI integration in Chinese cyber operations. By systematically recording and measuring attack parameters across repeated exercises, the platform generates the kind of data needed to train AI systems to eventually execute offensive campaigns with reduced or no human intervention. Experts consulted by Recorded Future news warned that combining large-scale reconnaissance of adversary networks with AI-driven attack optimization represents a significant and growing threat. Allar Vallaots, the chief operation officer at CR14—the Estonian cyber range used in NATO's Locked Shield's exercise, observed that "whoever possesses the better AI wins, because if an AI system attacks you, no human can defend it." Vallaots also explained that "if you can measure all the different parameters with an attack, then you train the attacks . . . you can take out the human error. AI can find paths, bottlenecks, other ideas, much faster than a human."

6. Platforms and Weapons Systems

6.1	**Deadly cargo: Chinese cargo ship packed with modular missile launchers** Images of a medium-sized Chinese cargo ship loaded with 60 containerized vertical launch cells, radar, and close-in weapons emerged in late December, revealing a long-discussed capability that could turn China's massive commercial shipping fleet into a significant and stealthy force-multiplier. (source) *Assessment:* The image of the vessel shows containers on its deck and large sensors, including a large rotating phased-array radar forward of the bridge atop three containers as well as another domed radar or communications system across the deck from it mounted on two containers. The ship also has a close-in-weapons system (CIWS). *The War Zone* states that the containerized vertical launchers are installed five wide and three deep, each packing four large launch tubes. This configuration gives the vessel 60 vertical launch cells, which is approximately two-thirds of the vertical launch system of an *Arleigh Burke* class Flight I or II destroyer. *The War Zone* reporting is careful to caveat the photo reveals by suggesting that there is no way to determine whether the capability is merely a mock-up, a concept demonstrator, or is further along in development. Regardless of the status of this specific vessel, China is not the only country to have demonstrated interest in containerized weapons. Lockheed Martin suggested the need for containerized launchers in April of 2025 and various military analysts have discussed the concept as an inexpensive means of achieving stealth, scale, and force survivability, including a February 2025 article published by the US National Defense University.

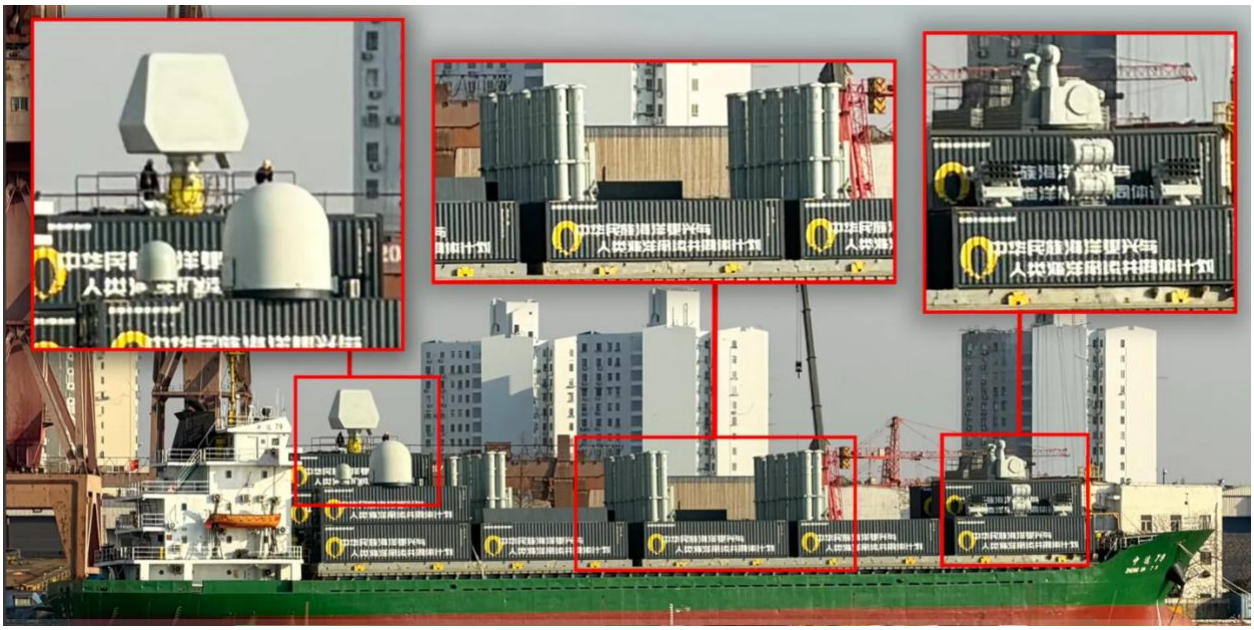

Figure 6: An image of the cargo ship carrying containerized missiles, radar systems, and CIWS. Source: Chinese internet via The War Zone

6.2	**Hellfire buggy: Ukraine successfully deployed Tempest military vehicle to shoot down drones** Ukraine's air defence forces claimed to have shot down at least 21 Russian Shahed drones with a new American-made light vehicle known as the Tempest that fires guided missiles from its back. (source and source) *Assessment:* Footage released by the Ukrainian armed forces in January featured multiple clips of the Tempest firing at night. Commentary from a Ukrainian soldier claimed the system has shot down 21 Shahed drones. The dune buggy-style vehicle has two missile launchers and a radar attached to its top used to launch Hellfire Longbow missiles. The soldier speaking on the video added that "this machine keeps the sky locked down." Other clips of the Tempest showed it moving in open fields and on roads. American company V2X manufactures the Tempest and stresses that the system uses commercial off-the-shelf components to keep costs down. As *Business Insider* noted, mobility is crucial for Ukraine's counter-drone efforts. Shahed drones fly at over 100 mph, leaving very little time for counter-drone crews to respond after a target is detected. Moreover, the number of Shaheds that Russia can produce and deploy—at relatively low costs—means that Ukraine needs lower cost munitions to counter the threat. While the Hellfire is more expensive than a Shahed drone, it is less expensive than other kinetic interceptors that can be used against fast-moving drones.

Figure 7: An image of the V2X Tempest from the Ukrainian video. Source: MilitaryNewsUA X

6.3	**Janes releases special report on North Korean nuclear-powered submarine** The submarine is described as a “nuclear powered strategic guided-missile submarine” and was revealed in late December 2025 following a visit by North Korean leader Kim Jung-un to an undisclosed shipyard. The new submarine would constitute a significant increase in undersea and deterrent capability. (source) *Assessment:* Janes describes the design of the submarine as “atypical” in comparisons to other ballistic missile submarines in service in other navies. An elongated sail dominates the vessel’s upper hull line and appears to house between eight and 10 vertical launch hatches. According to Janes analysis, modern ballistic missile submarines integrate launch tubes within the pressure hull rather than the sail to maintain structural integrity and hydrodynamic efficiency. However, the elongated sail design approach may make sense for North Korea as it allows the country to achieve its goal of accelerating efforts to field a nuclear-powered submarine launched ballistic missile capacity while still working within its technological constraints. Janes also notes that the design is like those used for Russian nuclear-powered ballistic missile submarines that entered service in the 1970s. The submarine’s size is also notable. With an estimated displacement of 8,000-8,700 tonnes, it is much larger than the Gorae-class experimental ballistic missile submarine, which Janes reports displaces roughly 1,500 tonnes. The size in conjunction with its nuclear propulsion will enable extended endurance and allow it to travel beyond coastal waters. While the main function of the submarine will be to serve as a deterrent and stealthily hold rival forces and infrastructure at risk, it does posses six horizontal torpedo tubes in the bow. This indicates that it retains a conventional attack capability.

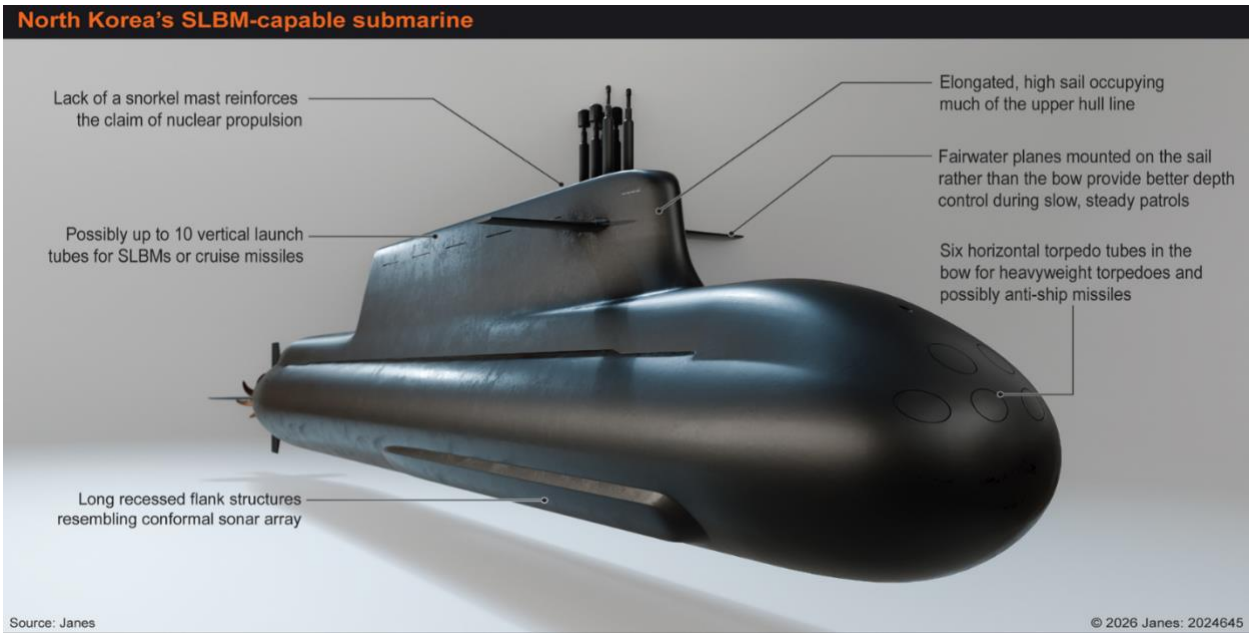

Figure 8: A 3D visualisation of North Korea’s SLBM-capable submarine, based on Janes analysis of images released by North Korean media organization KCNA between March and December 2025. Source: Janes

7. Sensors

7.1	**Can you hear me now? UK acquires acoustic detection system** Leonardo was awarded an £18.3 million contract to provide the British Army with the SONUS passive acoustic detection system as part of Project SERPENS. The system will allow British soldiers to more aggressively hunt, detect, and locate hostile fire. (source and source). *Assessment:* Project SERPENS is the British Army's effort to develop a next-generation weapons location system to replace older radar systems with advanced digitally networked sensors. Leonardo describes SONUS as the latest iteration of the company's Hostile Artillery Location (HALO) system. SONUS uses advanced acoustic processing to detect acoustic pressure waves from gunfire, mortars, and explosions, providing operators with a precise point of origin and point of impact. The system does not emit an electronic signature, which reduces the vulnerability of operators and allows SONUS to operate undetected. Another advantage of the system is that it is 50 percent smaller than the current iteration of HALO and 70 percent lighter, making it easier to transport, position, and conceal. It also requires reduced power consumption, extending its operational life. The system's software architecture is open by design. This will enable dynamic upgrades as well as integration with other systems. Acquisition of SONUS was accelerated by five years and is expected to be deployed with the 5th Regiment Royal Artillery within the next 12 months.


deftech.ch