Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

DEFTECH-SCAN

April 2026

OTH INTELLIGENCE GROUP

deftech.ch/scans

Dear Reader,

The current strategic environment is increasingly shaped by the convergence of geopolitical rivalry, rapid technological diffusion, and a steady expansion of competition into new domains.

States and non-state actors alike are adapting to a landscape defined by speed, scale, and ambiguity, where emerging capabilities are not only enhancing military effectiveness but also exposing new vulnerabilities across interconnected systems.

This edition includes a good range of stories that focus on the risks and operational opportunities associated with accelerating deployment of military AI; the vulnerability of civilian and military infrastructure in the homeland; the increased focus on building domestic defence industrial bases, the persistent challenges for Europe's defence industrial base as it attempts to scale and develop more independence from the United States, and the value of "useful fiction" and alternative analysis techniques to help build resilience in times of technological disruption.

As we prepare for what's next, take a look at these major news:

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@ar.admin.ch

1. Applications of AI and data

1.1	**The Gods of AI Warfare Revealed: Opportunities and risks of military AI** The on-going conflict in the Middle East has increased attention on the opportunities and risks associated with the deployment of AI-enabled decision support tools for military decision-makers and the ethical dilemmas associated with their use (source (firewalled) and source) *Assessment:* On 23 March, *Wired* published an excerpt from Katrina Manson's book *Project Maven: A Marine Colonel, His Team, and the Dawn of AI Warfare*. The article—entitled "Omniscience, Omnipresence, and Omnipotence: Meet the Gods of AI Warfare"—traces the story of the development of Project Maven from a controversial Pentagon experiment to a central pillar of modern U.S. military operations. The article argues that Project Maven's journey represents an historic shift toward rapidly advancing military trust in artificial intelligence to accelerate surveillance, targeting, and decision-making in war. Project Maven began in 2017 as an effort to use computer vision to process the enormous volumes of drone footage generated during America's counterterrorism operations. Analysts were overwhelmed by the amount of video collected, and the AI was viewed as a tool to more quickly and accurately identify objects, people, or suspicious patterns. After initial scepticism, the program found traction and, according to retired US Army Colonel Joe O'Callaghan who served as XVIII Airborne Corps Chief of Fires, became "a movement." The article recounts how Maven advocates overcame organizational inertia to build momentum for the program and adoption of it as a decision-support tool. However, its underlying message is as much ethical as it is technical, operational, or historical. The author's excerpt presents Project Maven as both a victory for military innovation *and* an increasingly urgent warning that militaries and the societies they represent are entering an era where machines may shape life-and-death decisions at unprecedented speed and scale. Both the opportunities and risks of AI were on display during the opening stages of Operation Epic Fury, the US attack on Iran and its leadership, which began on February 28, 2026. US Central Command conducted thousands of strikes, hitting more than 1,000 targets in the initial 24 hours alone, a pace that military leaders directly attribute to AI-assisted targeting systems. The opening strike against Iranian leadership targets lasted approximately one minute from decision to execution. Strike lists were updated within hours as satellite imagery and sensor fusion closed the sensor-to-shooter loop in near real time. However, the same acceleration that enabled unprecedented operational tempo also concentrates accountability risk with potentially tragic consequences. The US strike against a girl's school in Minab that killed between 170-180, most schoolgirls between ages 7-12, is reported to have resulted from outdated intelligence processed through Maven. *The Guardian* cited CNN reports that the US Defense Intelligence Agency had not updated its targeting database to reflect that the school had been separated from a military facility and converted into a school by 2016, at the latest. According to the *Guardian,* the failure was due to the dual facts that "People failed to update a database, and other people built a system [Maven] fast enough to make that failure lethal."

1.2	**US elevates AI to strategic risk** The US Office of the Director of National Intelligence's (ODNI) 2026 Annual Threat Assessment (ATA) frames AI not as a standalone risk but as a force multiplier reshaping global security dynamics across cyber, information, and military domains. (source and source) *Assessment:* For the first time, the ATA report treats AI as a central national security issue rather than a niche technology topic, describing AI as a "defining technology for the 21st century" that will shape military power, economic competitiveness, intelligence operations, cyber conflict, and geopolitical influence." The authors focus considerable attention on how China and Russia are leveraging AI to improve cyber operations, intelligence collection, and autonomous military systems, increasing the speed, scale, and precision of potential attacks. AI-enabled tools can automate cyber intrusions, enhance targeting, and reduce barriers to entry for sophisticated operations. The competitive dimension of the report centres squarely on China's military AI development. Beijing is assessed as the most capable competitor in the AI space, aiming to displace the US as the global AI leader by 2030, leveraging its talent pool, extensive datasets, government funding, and global partnerships. Advanced semiconductors are identified as the enabling foundation, with domestic chip design and production described as both an economic and geopolitical priority. The report also flags AI's role in the broader threat landscape, including its use by adversaries in cyber operations and its potential exploitation by terrorist actors for propaganda and radicalization, situating AI as a force multiplier for a wide range of threat actors, not just great-power rivals. At the same time, the ATA implies that the United States must harness AI itself to remain competitive. Intelligence agencies and the broader national security apparatus will need AI for data processing, predictive analysis, and decision support as global information volumes exceed human capacity. Overall, the 2026 ATA portrays AI as both an opportunity for US advantage and a threat multiplier for rivals, making technological leadership a core security priority for the coming decade.

1.3	**A common theme: Military AI for me but not for thee** Two reports during the period demonstrate that China's approach to AI development is, at least at a strategic messaging level, consistent with that reflected both by continued US development and deployment of AI and the ODNI warnings of the risks of AI developed and deployed by its chief rivals. (source and source (firewalled)) *Assessment:* In March, China's People's Liberation Army unveiled an AI-assisted aerial refuelling management system that, according to the *South China Morning Post,* represents a meaningful operational capability increment. The system monitors real-time airspace conditions, tracks fuel status across participating aircraft, and generates optimized pairing plans between tankers and fighters, improving the previously inefficient proximity-based process. The announcement occurred shortly after a US KC-135 crashed during operations linked to the Iran conflict and was framed as a superior solution to the operational strain placed on aging crewed systems that contributed to the US crash. However, while Beijing is actively increasing its efforts to incorporate AI into military systems, it is also running a strategically calculated influence campaign around military AI. Reporting from *The Diplomat* shows that beginning March 11, Chinese Defence Ministry spokesperson Jiang Bin began pushing a narrative portraying US military AI integration as leading toward a dystopian "Terminator"-like future. The campaign casts the United States as reckless while simultaneously positioning China as a responsible actor in global AI governance. *The Diplomat's* analysis argues this is less a sincere warning about AI safety than a deliberate exploitation of three converging vulnerabilities in the American information environment: • Western publics' tendency to import beliefs from fiction • The very public feud between the Trump administration and AI companies over military use, which is likely to deepen partisan polarization • Russia's historical playbook of using narratives to drive wedges between American groups rather than to be believed outright. The contradiction is stark and not entirely dissimilar—though perhaps more cynical—to the actions and assessments of the US government discussed above. China is rapidly integrating AI into its own military systems while publicly warning about the dangers of US military AI. This dual tract approach is not necessarily surprising, given the intensity of the competition to become global leaders in AI adoption and governance and the increasing importance militaries around the world are placing on AI. However, it does reflect a strategy of leveraging information operations to influence global norms without constraining national capabilities.

1.4	**AI radar: A new frontier in threat detection** India's Defence Research and Development Organisation is developing an AI-enabled radar to detect and track hypersonic missiles traveling at speeds exceeding Mach 5, potentially easing one of the most challenging problems in modern air defence and reflecting how AI is reshaping the future of detection and tracking. (source) ***Assessment:*** Hypersonic weapons traveling above Mach 5 are extremely difficult to track because they generate plasma envelopes that can degrade or block conventional radar signals. India's approach leverages AI-driven signal processing to overcome this challenge. Specifically, the Indian system counters this by combining an L-band Active Electronically Scanned Array, which operates at longer wavelengths less susceptible to plasma interference, with gallium nitride transmit-receiver modules for improved signal penetration. Critically, AI and machine learning are used to adjust the radar's settings in real time, including frequency ranges, pulse waveforms, and scanning behaviour, allowing the system to continuously adapt as the target shifts speed, altitude, and plasma characteristics during flight. The effort, along with growing investment in other AI-enabled radar systems, demonstrate how AI is reshaping the future of radar by enabling detection and tracking of faster, smaller, and more complex threats. AI is no longer a complementary capability for radars but rather a crucial component enabling radars to operate effectively in electromagnetically hostile and time-compressed threat environments in conflict.

2. Robotics and Autonomous Systems

2.1	**Institute of International and Strategic Studies (IISS) report assesses the impact of "uninhabited aerial vehicles" on deterrence** In March 2026 IISS published a Strategic Dossier on UAVs that provides an in-depth assessment of how unmanned aerial vehicles have evolved into foundational elements of military deterrence and combat power. (source) *Assessment:* The report includes chapters covering how select states in Europe, the Middle East, and Asia employ uncrewed aerial systems (UAS) for intelligence, surveillance, and reconnaissance (ISR) in support of deterrence and combat operations; UAS use in Russia's war in Ukraine; and how the selected countries are approaching the development and/or acquisition of collaborative combat aircraft (CCA). The report's central analytical argument is that ISR is no longer merely a support function but a core pillar of deterrence. Still, the Ukraine case study illustrates a structural limitation of deterrence by detection. Simply detecting adversary assets does not necessarily lead to dissuasion. Western ISR accurately characterized Russian intent before the 2022 invasion, but that intelligence did not alter Putin's calculus. Deterrence requires not just information advantage but credible capacity and political will to impose costs. The dossier's future-focused assessment identifies collaborative combat aircraft (CCAs), a topic frequently covered in DEFTECH Scans, as the next major inflection point in the development of military UAS and associated operational concepts. Programs are advancing in the U.S., UK, Europe, and Indo-Pacific, with some CCAs potentially operational by the early 2030s. Europe's ongoing struggles to develop a viable multinational MALE UAV platform are highlighted as a persistent structural vulnerability, reflecting tensions between national industrial ambitions and urgent operational requirements, which are discussed in more depth in section 3.

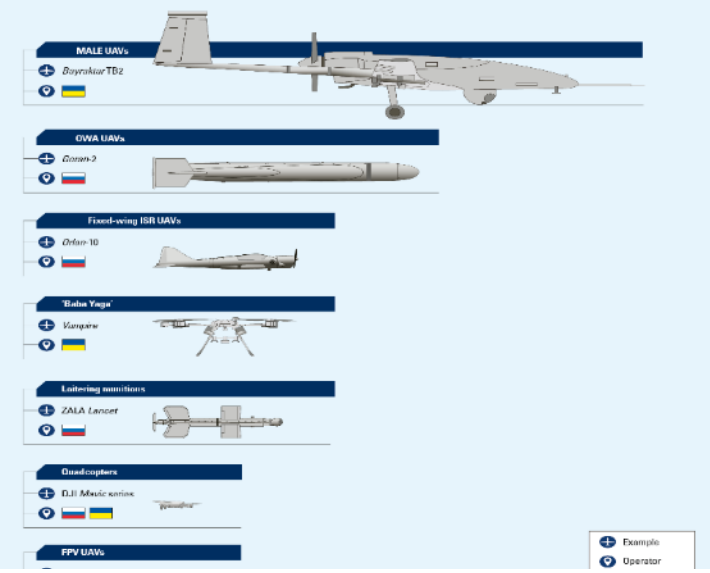

Figure 1: One of the 30 bespoke images and infographics included in the report. This image depicts key systems deployed in the Russia-Ukraine war. Source: IISS

2.2	**Drones over Barksdale: More mysterious drones flying over US military bases** Several waves of drones flew over Barksdale Air Force Base (AFB) in Louisianna. The base houses multiple legs of the US nuclear triad. The incident is one of a several recent reports of drones flying over military bases in the United States and elsewhere, including in France where mysterious drones overflew a nuclear submarine base at the end of 2025. (source and source) *Assessment:* Reporting from *Asia Times* describes repeated incursions of Barksdale's air defences by drone swarms composed of 12 to 15 drones per wave occurred during the week of 9 March. Each wave lasted approximately four hours. Barksdale is a strategically important base that houses the Global Strike Command, B-52H bombers, and nuclear cruise missiles. The drones displayed jam-resistant and likely autonomous behaviour, used non-commercial signal characteristics, and employed varied ingress and egress routes to resist triangulation. B-52 launches in support of Operation Epic Fury were reportedly delayed, marking what may be the first time a U.S. strategic air base was temporarily degraded during wartime. The Barksdale incident illustrates that homeland military installations are no longer beyond the reach of a determined adversary. Ukraine's impressive counter-drone adaptation in its ongoing war with Russia has closed the gap between offensive drone sophistication and defensive counter-drone capability on the front lines of an active and dynamic conflict. However, there clearly remains a gap in capability even in sophisticated militaries in homeland base defence. This vulnerability is not uniquely American. Reporting by the *Associated Press* on a series of drone overflights at a French nuclear submarine base in December 2025 underscores a broader and growing pattern: unidentified drones have repeatedly penetrated the airspace of one of France's most sensitive strategic sites, prompting security investigations but yielding limited public attribution or clear mitigation success. The incidents highlight how even well-defended nuclear facilities in advanced militaries are struggling to detect, track, and deter persistent drone incursions. Taken together, these cases suggest that drones are no longer merely tactical battlefield tools. They are increasingly capable of probing and even disrupting the most sensitive nodes of nuclear command, control, and force generation infrastructure.

2.3	**Turkey's Baykar unveils kamikaze drone capable of autonomous swarming** The K2 next generation autonomous swarming attack drone constitutes an interesting capability that sits at the seam between drones and cruise missiles and is designed to take advantage of growing global demand for drone swarms to saturate modern air defences. (source and source) Assessment: Turkey's Baykar unveiled the K2 kamikaze UAs on March 14, 2026, following multi-day autonomous swarm flight tests over the Gulf of Saros. According to Baykar: "The platform, featuring multi-operation capabilities and advanced AI and autonomy algorithms, successfully completed formation flight tests with 5 aircraft in varying configurations." The platform has a maximum take-off weight of 800 kg, carries a 200 kg warhead, has a range exceeding 2,000 km at speeds above 200 km/h, and endurance beyond 13 hours. These specifications place the K2 at the high end of the loitering munition spectrum and into territory that overlaps with cruise missiles rather than conventional tactical drones. The K2 is designed to operate in GPS-denied and electronically contested environments, using a gimballed EO/IR sensor to visually scan terrain features for position estimation, and supporting both line-of-sight and beyond-line-of-sight satellite datalinks. The K2's debut is significant on at least two levels. First, Baykar explicitly frames the K2 as designed for mass production at low cost to enable cost-effective neutralization of critical targets at a lower cost than cruise missiles. Second, the system has been designed with an eye toward the export market. Baykar recorded $2.2 billion in uncrewed combat aerial systems (UCAS) exports in 2025, with nearly 90 percent of revenues from international sales across 37 countries, meaning the K2 could rapidly proliferate to a wide range of state actors. A future reusable variant with a separable warhead is also in development, which would shift the K2 closer to a multi-mission strike UAV. Some analysts have pushed back on Baykar's claim of achieving a combat or export ready capability, noting that the company's tests included only five-drone formations, which is significantly smaller than emerging visions of a military swarm capability. Moreover, some point out that the trials did not appear to simulate a representative contested environment. Nonetheless, the K2's emergence reflects two important trends shaping the future of combat and military capabilities. First, it captures the growing global interest of militaries around the world in employing drone swarms as a means of overwhelming improving air and missile defences, especially swarms that can operate in contested electronic warfare environments. Second, and more abstractly, the K2's combination of size, range, speed, and endurance and low-cost production approach offers another example of how former distinctions in different capabilities—such as cruise missiles and drones—is blurring in many important ways.

Figure 2: Three images of the K2 during its March tests. The top image gives some concept of the drone's size as the swarm taxis on the runway before take-off. The middle image shows the five-drone swarm in formation. The bottom picture shows the drone's wingspan and payload. Source: Baykar YouTube video

3. Manufacturing and Industry

3.1	**Europe's 6th generation fighter programmes struggle to reach altitude** Recent reporting shows that Europe's flagship sixth-generation fighter programs—the UK, Italy, Japan Global Combat Air Programme (GCAP) and the France, Germany, Spain Future Combat Air System (FCAS)—are both facing significant political and industrial strain.(source, source (firewalled), source, and source) *Assessment:* While the overall health of the GCAP program appears to be in better shape than FCAS, tensions have emerged among partners at two levels in recent months. First, Italy's defence minister Guido Crosetto sharply criticized the UK for excessive secrecy around the program, calling the situation "madness" and warning that limited information-sharing risks undermining trust among partners. He told reporters in January that he had "ordered Leonardo to share its technology" to set an example of transparency and technology sharing that the other partners could follow. Second, in March, *Financial Times* published a report indicating that Japan had become concerned about repeated delays to the UK's defence investment plan. These delays are preventing the signing of a vital contract for design and development work with Edgewing, the commercial joint venture between the three nations' leading defence contractors: BAE Systems, Leonardo, and Mitsubishi Heavy Industries. An anonymous source involved in GCAP referred to the hold-up of project work caused by the UK delays as "a terrible situation." The *FT* reporting also stated there were competing visions about the nature of the capability being produced. The challenges facing FCAS appear even more acute. Multiple reports describe escalating conflict between Dassault Aviation and Airbus over leadership of the fighter aircraft component, the program's core element. Disputes over intellectual property, industrial roles, and control of design authority have plagued the program for years. In early March, Dassault CEO Eric Trappier bluntly warned that "if Airbus maintains its position of not wanting to work with Dassault, then the project is dead." Paul Taylor of the European Policy Centre described the project in February 2026 as having been clearly "dead for a year or two," stating that "it just won't lie down, because it's a political project". Despite these industrial challenges, political leaders have resisted that conclusion. At the 23-24 EU Summit in Cyprus, French President Emmanuel Macron denied the programme was dead and confirmed that he and Chancellor Merz had tasked their defence ministries to continue working on several areas of the €100 billion project. Across both programs, there is a consistent underlying pattern and theme. Ambitious multinational efforts to develop next-generation airpower are colliding with national industrial interests, sovereignty concerns, and differing operational requirements. While GCAP and FCAS aim to deliver advanced, networked combat systems by the 2030s and 2040s, their progress is increasingly shaped not just by technology, but by politics and competing visions of control that are unlikely to dissipate despite the increasingly fraught global security environment.

3.2	**European defence at a crossroads: Reducing dependence will take time** Europe is simultaneously grappling with the urgent need to rebuild its defence industrial base and confronting the stark reality of how far it still must go. These two pressures are captured in a European Commission announcement and a *Defense News* survey that was published during the reporting period. (source and source) *Assessment:* On 29 March, the European Commission announced the adoption of a €1.5 billion work programme under the European Defence Industry Programme (EDIP). The EDIP programme provides €1.5 billion in grants for 2026–2027, targeting production increases in key defence components including counter-drone systems, missiles, and ammunition. Of this, more than €700 million is directed at boosting industrial output, while €260 million flows through a Ukraine Support Instrument to help rebuild and modernize Ukraine's own defence technological and industrial base. Defence start-ups will also receive equity support worth €100 million collectively, as part of an initiative to accelerate defence supply chain transformation. The programme marks the first time Ukraine has been included as a partner in an EU defence industrial initiative, a recognition of how deeply the war has integrated Ukrainian and European security interests. Yet the *Defense News* survey of 16 European security analysts makes clear that money alone cannot close the gaps quickly. Europe will need until the early 2030s to develop some critical defence enablers, with robust air and missile defence potentially taking five to ten years to establish. Space-based ISR and integrated air and missile defence are the areas of greatest pessimism among analysts surveyed, with half expecting those capabilities to remain insufficient for more than five years. François Heisbourg, special adviser at the Paris-based Foundation for Strategic Research captured the scale of the challenge, assessing that, “there are areas in which the Europeans have zero meaningful capability, there are a few areas in which the Europeans own an arguably adequate capability today but for which the issue is one of replacement, and there some areas in which scale, not quality, is the issue,” The dependence on American command-and-control, deep strike, and satellite intelligence is particularly acute. Without American command and control, Europe would struggle with coordinated and distributed fires during operations, according to the *Defense News* survey. The EDIP investment and the capability audit together tell a coherent story. Europe has recognized the problem and begun to act, but the industrial and operational gaps are wide enough that the continent remains dependent on American enablers for the near term. Translating spending into fielded, integrated capability at scale, and in time is the central challenge of European defence over the next several years.

3.3	**Japan "accelerates" defence industry and defence technology ecosystem development** Three significant developments during the reporting period reflect Japan's continued efforts to normalize and modernize its defence and national security policy posture, moving to support innovation in defence technologies and offer more opportunities for startups and commercial companies to join the country's defence industrial base. (source, source, and source) *Assessment:* Japan's long-standing separation between civilian innovation and military capability is eroding through a coordinated set of policy, industrial, and international decisions that constitute a deliberate national strategy to build a modern defence technology ecosystem. At the policy level, Tokyo's newly adopted Five-Year Science and Technology Plan (FY2026–2030) marks a clear doctrinal shift. The document, released in late March, explicitly promotes dual-use R&D, elevating AI and semiconductors as "national strategic technologies" and calling for new institutional mechanisms to guide critical technology development. This reflects a recognition within Japan's defence and policy communities that technological advantage in areas like AI-enabled decision-making and advanced computing is vital for military operations and broader concepts of national security. The move is also shaped by external pressure, including Chinese export controls on rare earths and other dual-use inputs, which have underscored Japan's vulnerability across both civilian and defence industrial supply chains. That policy shift is now being operationalized through industry. On 9 March, Fujitsu announced the launch of the country's first dedicated defence-tech accelerator under contract from the Acquisition, Technology & Logistics Agency (ATLA). This move represents a structural bridge between government requirements and the commercial innovation base. Its focus on agentic, multi-AI decision-support systems places Japan in the global race to integrate AI into command-and-control architectures. More importantly, the accelerator's "open innovation" model signals that this model is designed to be a repeatable pipeline not just a one-off initiative, effectively creating a pathway for startups and non-traditional players to enter the defence sector. At the same time, according to 5 March reporting from *Nikkei Asia*, Japan is seeking to internationalize this emerging ecosystem. Discussions with NATO to join the Defence Innovation Accelerator for the North Atlantic (DIANA) would, if successful, give Japanese startups access to a transatlantic network of test centres, funding channels, and procurement pathways. This would not only accelerate the scaling of Japanese defence technologies but also embed Japan within a broader allied innovation architecture spanning Europe and North America. Taken together, these developments point to a coherent strategic trajectory. Japan is systematically dismantling postwar constraints that kept defence and commercial technology ecosystems apart, while simultaneously building domestic capacity and integrating with allied innovation networks. The result is an emerging model in which policy reform, industrial mobilization, and international collaboration reinforce one another, positioning Japan as a more consequential player in the global defence technology landscape amid intensifying great-power competition.

4. Human Protection and Performance

4.1	**Havana Syndrome update: US tests Russian weapon** The US Department of Defense tested a directed energy device obtained from a Russian criminal organization that appears to create similar effects to those associated with the mysterious "Havana Syndrome", which has afflicted US diplomats around the world since 2016 (source and source) *Assessment:* "Havana Syndrome" refers to a set of unexplained neurological symptoms, such as dizziness, headaches, cognitive disruption, and auditory disturbances that were first reported by US diplomats in Havana in 2016. Early speculation about the origins of Havana Syndrome focused on the potential of directed energy weapons being used against US diplomats and members of the US intelligence community abroad. However, a 2022 US intelligence assessment judged that most cases were unlikely caused by a foreign adversary, reinforcing a narrative that the phenomenon was either environmental, psychological, or otherwise non-weaponized. Two recent reports from CNN and *The Defense Post* mark a shift in that narrative. According to these accounts, the Department of Defense spent more than a year testing a device obtained through an undercover operation for roughly $15 million from a Russian criminal network. The device is portable, backpack-sized, and built with Russian components and emits pulsed radio-frequency energy. U.S. military laboratory testing on animals produced neurological effects and tissue damage patterns consistent with symptoms reported by affected personnel. The existence of a physically validated device capable of replicating these effects does not resolve attribution or confirm that past incidents were deliberate attacks. However, it significantly strengthens the case that the underlying mechanism long hypothesized is both scientifically plausible and operationally feasible. Most concerning is the implication of proliferation. If such technology is viable in a compact, deployable form—and possessed by a Russian criminal gang willing to sell it—it may already be accessible to multiple state and non-state actors.

4.2	**Monitoring soldier brains to optimize readiness and performance, but at what cost?** The US Air Force is working with a startup to develop a headset to monitor cognitive fitness of its personnel to reduce fatigue, sharpen focus, and improve performance. Neuro-ethicists have raised concerns about several challenges associated with the systematic collection of brain activity data. (source and source) *Assessment:* A $1.2 million Air Force partnership with consumer neurotechnology startup Neurable illustrates the Pentagon's expanding investment in AI-powered brain-computer interfaces and the continued efforts to develop data about soldier, sailor, airman, or marine mental and cognitive status to optimize performance. The project involves electrode-studded headphones that track service members' cognitive fitness by mapping brainwaves against markers of focus, alerting users when attention is flagging and providing neurofeedback to train toward peak performance. The broader Pentagon investment in the $3 billion BCI market includes helmets, earbuds, and other wearable devices using AI to interpret brain signals. According to Neurable's website, the company's headphones are used commercially by individuals engaged in mentally stressful activities, especially video-gaming, to track brain activity and improve focus and reduce burnout. The company's main product is the MW75 Neuro LT headset, pictured below. While the potential benefits for military readiness and personnel well-being could be significant, the ethical concerns about the tracking of cognitive data are extensive and not effectively addressed by existing law. Only four U.S. states afford legal protection to neural data, and neither international human rights law nor federal regulations safeguard mental privacy or neural autonomy. Experts raise concerns about algorithmic discrimination, adversarial hacking of implanted devices, and the long-term identifiability of anonymized but highly personal brain activity data. James Giordano of the National Defense University warned that enforced use of such devices could create a "very dystopian basis for behavioural control."

Figure 3: The Neurable MW75 Neuro LT. Source: Neurable MW75 Neuro LT product page

5. Connectivity

5.1	**Switzerland to modernize electronic warfare capabilities** Switzerland is advancing a modernisation of its electronic warfare capabilities under the Insigne programme, formally announced by armasuisse on 12th February 2026. Insigne will enhance the Swiss armed forces' electronic attack and electronic support capabilities. (source) *Assessment:* Switzerland's Insigne programme represents a significant technological upgrade to its electronic warfare (EW) capabilities, cantered on networked, modular, and interoperable systems. Led by Armasuisse, the programme will deploy distributed Electronic Support Measures (ESMs) that can detect, locate, and identify electromagnetic emissions such as radar signals. These sensors will be linked to electronic attack systems, primarily jammers, capable of disrupting or neutralizing those threats. The key technological feature of Insigne is its networked architecture. ESMs, jammers, communications links, and command-and-control (C2) systems will be integrated into a unified system capable of generating a "recognized electromagnetic picture." This shared operational view allows for faster detection-to-response cycles and improved coordination across military units. Supporting software will enable electromagnetic order-of-battle management, data analysis, and real-time intelligence dissemination. The system is designed with modularity and adaptability in mind, allowing components, both sensors and effectors, to evolve alongside emerging threats. Insigne also emphasizes interoperability, ensuring seamless data exchange with existing Swiss systems such as the FLORAKO air defence system and future platforms like the F-35A Lightning II. Technologically, Insigne builds on existing capabilities, including mobile SIGINT platforms and static sensor networks, but enhances them through connectivity, automation, and joint-force integration. The result is a more agile, data-driven EW ecosystem capable of operating across tactical, operational, and strategic levels.

Figure 4: A visual depiction of the Insigne programme from Armada International

5.2	**Flipping the script: Useful Fiction posits quantum computing as cyber curtain** *Defense One* published a scenario-based FICINT piece from *Ghost Fleet* authors Peter Singer and August Cole entitled "The Quantum Curtain" that explores the potential for quantum computing to radically strengthen cyber security. (source) *Assessment:* The piece was written in support of NATO's Allied Command Transformation and is built around a fictional January 2033 memo from the US National Security Advisor to the US president. The memo describes a breakthrough in a Quantum Key Distribution (QKD) satellite communications network called the Harpocrates system. The memo states that the system is a constellation of 210 CubeSats and an unknown number of easily portable receivers. The QKD communications technology underpinning Harpocrates is "based on a laser-like ground-satellite-ground transmissions; in this case single photons used at optical frequencies that work similarly to laser communications." The capability, access to which has proliferated widely after the inventor released technical details through various open-source innovation communities, makes it impossible for quantum encrypted messages to be intercepted. If a message is intercepted, its integrity is compromised in a way that is obvious to both sender and recipient, providing an exceptionally high degree of protection against cyber and electromagnetic spectrum operations. The fictional memo makes the operational stakes of Harpocrates clear by listing specific challenges that increasing access to the system poses for specific operations and meetings: • The delay of an operation to capture the head of ISIS Afghanistan-Pakistan because the US military is no longer able to access ISIS-APK communications due to their use of the QKD capability. • Degraded ability of the US Navy to track People's Liberation Army Navy (PLAN), maritime militia, and Chinese Coast Guard vessels in the South China Sea due to the use of Harpocrates on several ships, which are then communicating with ship-to-ship laser-burst transmissions fleetwide. • Inability to obtain information about Russian positions on key issues of negotiation in advance of an upcoming US-Russia Presidential Summit, as Russia's president's inner circle has begun using Harpocrates as well. Singer and Cole's piece is interesting both for its form as well as its message. In an environment marked by disruption, uncertainty, and rapid technological advancement and diffusion, the ability to think creatively about the future and future outcomes is essential to building resilience and identifying both risks and opportunities. Scenario planning, wargaming, useful fiction/fictional intelligence (FICINT) offer creative means of expanding analytical filters and exploring the future while not necessarily being tied to a single outcome or pathway. The piece is also interesting due to its focus on the impact of QKD to protect communications and reduce the capacity of modern militaries to collect the information required to maintain situational awareness. As the memo concludes: Harpocrates constitutes a "potential breakpoint in our access to the scale and quality of information that we depend on" to deter, dissuade, monitor, and defeat adversaries.

5.3	**Germany to explore free-space laser communications with Elbit Systems** Elbit Systems Deutschland signed an agreement with German startup Cucuyo GmbH to develop laser-based communications technology for defence. (source and source) *Assessment:* Free-space optical (laser) communication transmits data via light rather than radio frequency (RF) signals. This approach offers several technological advantages: faster transmissions, significantly higher data throughput, resistance to electronic warfare jamming, and a low probability of interception due to the narrow, non-emitting beam. These features are particularly relevant for next-generation, data-intensive platforms such as drones, distributed sensor networks, and satellite networks. Elbit is establishing a dedicated R&D organization to mature these capabilities, initially focusing on integration with unmanned aerial systems and ground platforms. The technology itself is described as lightweight and high-performance, designed to enable "secure, high-capacity data links" critical for modern operations. Company leadership underscores both the technological and strategic implications. Elbit Deutschland CEO Marian Rachow noted that developing advanced technologies in Germany for NATO use is a "cornerstone" of Elbit's strategy, adding that the partnership reinforces "commitment to investing in German innovation." Meanwhile, Cucuyo CEO Frank Negretti emphasized the breakthrough in form factor and capability, stating the collaboration will deliver "a compact, UAV-compatible format – with high capacity and long range."

Figure 5: A depiction of how laser-based communications can connect uncrewed systems in a more secure and faster way. Source: Elbit Systems and Cucuvo GmbH

6. Platforms and Weapons Systems

6.1	**Lasers take to the skies: Elbit contracted to put lasers on military aircraft** Elbit Systems has revealed in March that it received a contract from the Israeli Ministry of Defense to mount a high-powered laser weapon on military aircraft, extending the range and improving the efficiency of laser-based air defences compared to ground-based weapons (source) *Assessment:* CEO Bezhalel Machlis disclosed the late-2025 deal during the company's annual investor meeting, presenting two platform-specific variants: XCalibur for fixed-wing aircraft and Sting for helicopters. Machlis framed the technology as a cost-effective answer to modern asymmetric threats, arguing that using expensive interceptor missiles against cheap drones is "unsustainable." Instead, lasers allow operators to spend what he referred to as "cents of electricity" to defeat incoming threats. A key advantage of the airborne laser, Machlis noted, is that it is "less affected by humidity, rain, dust, atmospheric conditions the higher you go", enabling it to operate above cloud cover and engage threats at greater range than ground-based systems. He acknowledged significant engineering and operational hurdles, stating: "You need to miniaturize the elements. While moving, you need to lock yourself on a target and in a very precise way." However, Machlis said Elbit has managed to overcome all these challenges. Investor conference footage showed the laser destroying a missile, downing a Shahed 136-type kamikaze drone, and firing from a Black Hawk helicopter door. Machlis also hinted at offensive potential, noting the laser "is not just a defensive weapon" without elaborating. The airborne system would complement Rafael's ground-based Iron Beam, which was declared operational in December 2025. The strategic logic for putting lasers on aircraft is clear. Flying above cloud cover would extend effective range and allow threats to be neutralized farther from Israeli territory. The transition from experimental to deployable airborne laser warfare is likely to accelerate a broader shift toward scalable, low-cost counter-drone and missile defence architectures across advanced militaries globally.

Figure 6: A screenshot taken from Elbit CEO's presentation at the company's Investor Conference in March 2026. The image depicts the company's vision for the Sting and XCalibur systems operating in conjunction with the Iron Beam ground-based system. Source: Elbit YouTube

6.2	**Under the sea: The continued conflict along the seabed** Reporting from BBC and Associated Press in April highlights growing concern over Russian undersea activity in the North Atlantic, particularly around critical communications infrastructure. (source and source) ***Assessment:*** A joint British–Norwegian military operation tracked and deterred three Russian submarines, including an attack submarine and two specialized "spy" vessels known as GUGI submarines operating near undersea cables. The month-long effort involved a Royal Navy frigate, surveillance aircraft, and hundreds of personnel, forcing the submarines to withdraw without damaging infrastructure. Officials warned that Russia may be exploiting global distractions, such as conflict in the Middle East, to increase covert maritime activity targeting Europe's vulnerable seabed infrastructure. The BBC report adds broader context, emphasizing the strategic importance and fragility of undersea cables, which carry the vast majority of global internet and financial data. These cables are difficult to monitor and repair, making them attractive targets for espionage or sabotage. Western officials increasingly suspect that Russian naval units are mapping and potentially preparing options to disrupt these networks in a crisis. This activity is often framed as part of "grey zone" or hybrid warfare, where actions remain below the threshold of open conflict but still impose strategic risk. The two smaller spy subs are known as GUGI submarine. The acronym stands for the Russian words for Main Directorate for Deep Sea Research (Glavnoye upravlenie glubokovodnikh issledovanii). The organization is part of the Russian navy, though the BBC describes it as being "so secretive that it reports directly to the defence minister and the president." The GUGI mini subs can be launched covertly from other Russian military vessels and reportedly retain the ability to cut cables or interdict them to allow Russia to monitor the data passing through them. Together, the articles underscore a shift in focus toward seabed warfare, which Deftech Scans have previously highlighted. While no confirmed sabotage occurred in this case, the combination of persistent Russian undersea operations and the West's heightened surveillance response reflects a growing recognition that control of, and access to, he ocean floor's data infrastructure is becoming a critical domain of geopolitical competition.

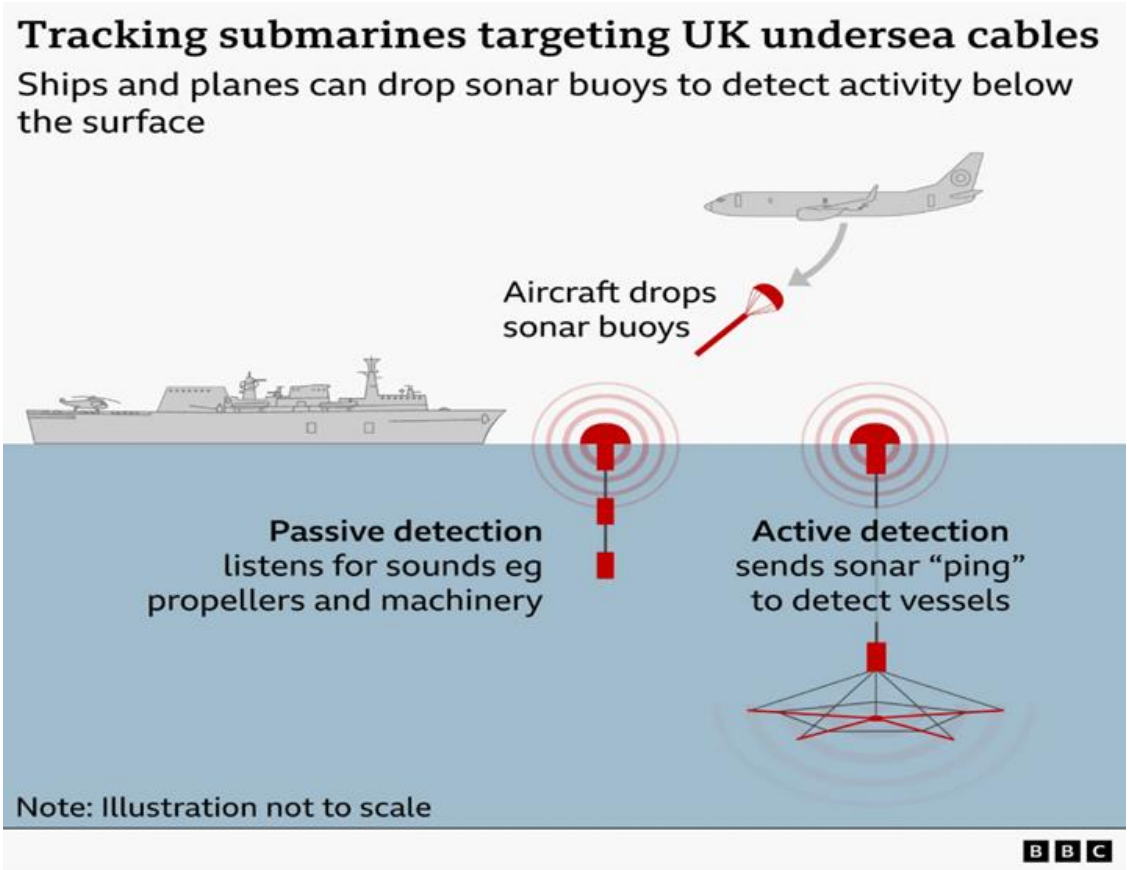

Figure 7: A BBC graphic showing how British and Norwegian forces are tracking Russian seabed military activity. Source: BBC


deftech.ch