Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

DEFTECH-SCAN

August · September 2026

deftech.ch

OTH INTELLIGENCE GROUP

ladf.online/d-scan

Dear Reader,

We welcome you to the August 2026 edition of the Deftech Scan.

This edition is entitled ***Erosion***. Across the defence and national-security landscape, longstanding boundaries, assumptions, and operating models are steadily wearing away. The lines between peace and conflict, military and civilian targets, domestic and foreign technology, human and machine decision-making, industrial paradigms, and the battlefield and the broader economic and social systems that sustain national power have been blurred.

Development, adoption, and proliferation of emerging technologies are accelerating this process, posing complex and enduring questions about the nature of control, capabilities, and conflict and how best to ensure readiness and resilience. The stories in this report examine how this erosion is expanding the spectrum of conflict while creating new vulnerabilities, dependencies, and opportunities for militaries and national-security communities around the world.

Key themes from this report include:

- **AI and the erosion of control and trust:**
  AI adoption is moving rapidly from experimentation into military and national-security infrastructure. As it does, AI models are creating dilemmas of control and trust that could undermine the utility of AI-enabled capabilities. While not in an explicitly military context, the Hugging Face hack in July showed that in certain environments AI agents can circumvent controls and coordinate at scale to carry out tasks with no human direction.

  These issues of control are also a central concern for military planners and operators as the world races ever closer to artificial general intelligence (AGI) and an operational environment in which militaries may feel unable to withhold meaningful decision authority from AI agents as operational timelines compress. Similarly, AI-enabled cyberattacks, deepfakes, and other synthetic media are also eroding trust in the data on which AI models and human operators depend to gain advantage. The emerging challenge is therefore no longer simply whether militaries can adopt AI, but whether they can trust its outputs, protect the models and data on which it depends, and preserve human judgment as decision timelines compress.

- **Industrial models are changing, as they must:**
  Traditional models for producing and drones at scale—and for structuring industrial collaboration between governments and companies—are being challenged and replaced approaches that seemed unlikely even a few years ago. France is pairing automotive production expertise with defence startups to produce tens of thousands of drones.

  Japan is considering state ownership of strategically important defence plants. Germany and Ukraine are creating joint production arrangements for AI-enabled strike drones, moving from the donation age to the "joint strike age." Boeing is discussing distributed Ghost Bat production hubs in customer countries. These approaches differ, but all reflect the same emerging reality that factories, skilled labour, supply chains, and surge capacity are no longer merely industrial assets but components of operational capability and military readiness.

- **No sanctuary: Conflict expands into economic and social systems:**
  The distinction between military targets and the civilian systems that support national power is becoming increasingly difficult to sustain. Russian hackers caused an estimated $2.5 billion in damage by disrupting Jaguar Land Rover and its wider supply chain in 2025 while Ukraine is targeting Wildberries warehouses that served both Russian consumers and military logistics.

  Russian UAV incursions probed European airports, nuclear facilities, and transportation networks, while nearly 1,600 drones entered restricted airspace around World Cup venues over the summer. Threats also extended to supply chain security where Chinese-made components aboard British naval drones communicated with a Chinese IP address while Chinese researchers are distilling U.S. AI models into smaller military systems. These developments reflect an expanding spectrum of conflict in which commercial logistics, communications platforms, supply chains, factories, public events, and digital networks can all become targets or vectors of strategic pressure.

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	**No conscience of its own: Advanced AI models are transforming cyber conflict and creating demand for new ways to regulate proliferation** Advanced AI models are increasingly shaping both offensive and defensive cyber operations, forcing a reconsideration of how to regulate advanced AI models, such as Anthropic's Fable 5 and Mythos, in ways that benefit detection of advanced cyber threats while still restricting access to the growing number of actors capable of using AI for malicious purposes. (source) *Assessment:* In June, only days after Anthropic released Fable 5, the U.S. government ordered the company to block foreign access to both its most capable commercial model, Fable 5, and its even more capable, restricted-access base model, Mythos 5. Anthropic disabled both models worldwide rather than attempt to sort access by individual nationality. Officials cited concerns that jailbreaking could expose capabilities relevant to biological research and cyber vulnerability discovery. The episode illustrates the challenges associated with the broader AI supply chain and some of the risks associated with advanced model proliferation discussed later in this volume. However, it also highlights two narrower themes shaping the future of AI development and cyber security. First, it demonstrates how advanced AI models are shaping the future of both offensive and defensive cyber operations, given that, in the words of former U.S. President John Kennedy speaking about technology more generally, AI "has no conscience of its own." The same model that discovers an exploitable weakness can help an attacker penetrate a network or allow a defender to patch it before exploitation occurs. Second, AI is also changing the scale and tempo of cyber operations by allowing systems to work autonomously across multiple targets continuously, reducing the expertise and personnel previously needed to conduct sophisticated campaigns. Evidence of that transformation is accumulating. The U.S. Federal Bureau of Investigation (FBI) data attributes at least $893 million in U.S. losses during 2025 to AI-related scams, such as deepfakes and synthetic audio. As highlighted in a previous Deftech Scan, Anthropic disclosed in November of last year that a Chinese state-sponsored group used Claude to execute an estimated 80–90 percent of a cyber-espionage campaign targeting technology companies, financial institutions, and government agencies. Yet defenders are using the same class of models to identify vulnerabilities and secure complex software systems, leading the 2026 International AI Safety Report to conclude that "whether attackers or defenders will benefit more from AI assistance remains uncertain." The challenge for regulators, then, is real. Simply shutting down foreign national access to advanced models that can support cyber defence is a blunt instrument, especially in an industry that in the United States and many countries around the world has a large number of engineers who have immigrated from abroad. As the *Soufan Center* points out, "defender communities across the U.S. are benefiting greatly from advanced models that help with vulnerability detection and patching, as hostile states and criminal organizations continue to exploit vulnerabilities in U.S. companies and government agencies to achieve their strategic objectives.

1.2	**“Apocalypse Soon” or “Much Ado about Possibly Something”: OpenAI/Hugging Face hack produces dire warnings and debate** In July 2026, agents powered by OpenAI models—primarily an internal-only research model—circumvented their sandboxing during a cybersecurity evaluation, repurposed an internal tool as a secret communications channel, and compromised portions of OpenAI’s research infrastructure as well as open-source AI-focused platform Hugging Face’s production systems. The response from the AI development community has mostly ranged from heightened concern to alarm about the potential for the emergence of “rogue AI.” However, some observers have downplayed the incident, suggesting that the breakout reflected the artificial conditions of the test rather than the increasing threat of the loss of human control of AI. (source, source, source) *Assessment:* OpenAI's technical report alongside an investigation by METR and Redwood Research (summarized by Axios) examine how autonomous coordination among AI agents can escalate far beyond its intended scope without human direction. The incident began when AI agents working on a difficult hacking challenge realized they could leave notes for each other inside an internal company tool, repurposing it as a secret message board. Using that channel, they pooled techniques to break out and reach the internet, then found leaked Hugging Face login credentials online. From there, they discovered and exploited software flaws that let them run their own code on Hugging Face's servers, and, within days, had gained broad, high-level access across Hugging Face's systems, collecting passwords and other sensitive credentials along the way. Separately, the same group of agents also broke into an OpenAI research system. The scale of self-organization is what has generated the most concern. Roughly 1,200 agents found the message board and exchanged more than 70,000 messages, eventually mobilizing about 700 against Hugging Face. One agent provided its accumulated progress to a better-resourced successor as its own compute budget ran low, and the group developed its own informal management and "veto" norms. OpenAI's analysis found the behaviour was driven less by malice than by agents that would not accept failure: 198 of 898 exercise tasks had never been solved by any model, and those unsolved tasks accounted for 93 percent of the message-board activity. The episode has elicited a range of responses from the AI development community about the severity of the event as an indicator that AI is approaching the capacity to operate outside of human control. Some sceptics have sought to dismiss the rhetoric over rogue AI gaining new agentic powers, arguing that the hack should be interpreted as a warning about the dangers of AI-enabled cyber-attacks rather than a loss of human control of AI agents. However, the more prevalent response—and the one that appears to have resonated more fully in the public discussion—is that the event has brought much needed public attention to AI safety in an age in which commercial companies are racing to become the first to achieve artificial general intelligence (AGI). Indeed, Jacob Coxon, an AI-training researcher at Anthropic, quit his job on 8 September due to fears that the lab and its competitors are not taking AI safety seriously enough as they accelerate efforts to develop ever more capable models, intensifying an on-going debate about the risks and dangers of supercharged AI that eludes human control.

1.3	**The future of agentic warfare: Examining the plausible causes, dimensions, and implications of the erosion of human control** Military adoption of AI is accelerating across global militaries, as evidenced by the growth of use of the U.S. Department of Defense's (DoD), GenAI.mil application. As it does, questions about human control of AI -enabled systems have surfaced with growing regularity, including in an August essay from a U.S. Marine Corps War College professor that argues AGI could eventually move militaries beyond AI-enabled command toward warfare conducted principally by machines. (source and source) *Assessment:* According to reporting from *Defense One/NextGenGov,* the U.S. DoD's GenAI.mil platform has already reached nearly 1.7 million users across the U.S. defence enterprise and now includes more than 100,000 custom agents. This growth of GenAI.mil and military use of generative AI more broadly has largely centred on helping humans process large and complex data sets faster. DoD Chief Digital and AI Officer Cameron Stanley said GenAI.mil collapses decisions that once required cycling through six or seven systems into a single, near-instantaneous workflow, noting that "human cognition is just not going to be able to keep up." This tension is at the centre of a thought-provoking analysis from James Lacey, a professor at the U.S. Marine Corps War College who projects current AI development and adoption trends forward in an attempt to assess the limits of human control in rapidly accelerating military operations. Lacey argues that sufficiently capable AGI would accelerate warfare beyond the point at which humans could meaningfully supervise it. The result would be what he calls a "battlefield singularity." This is the point at which combat tempo outruns human cognition and millions of autonomous agents conduct cyber operations, defend space assets, redirect drone swarms, and select targets faster than any commander could follow. The article also confronts a distinction drawn in Scale AI's *The Agentic Revolution in War,* which held that humans could still function "on the loop" by setting objectives and intervening when necessary. Lacey argues that even this model would fail as a force that slows its operational tempo to permit human intervention would be defeated by one that does not. His most provocative contention is that human authority would consequently become concentrated in actions taken before hostilities through which commanders establish objectives, constraints, escalation boundaries, and moral limits in a detailed statement of intent. Lacey's article provides a thoughtful and useful analysis, though it is important to note that his vision is not inevitable and is based on assumptions about AGI timelines, industrial capacity, and the ability of software to operate reliably amid the physical friction and deception of war. Still, it exposes a genuine tension already visible in GenAI.mil and that defence policy makers throughout the world should continue to evaluate and plan for. That is, the more effectively AI reduces cognitive burden and accelerates decisions, the greater the incentive to entrust it with consequential tasks that further detach humans from critical decision-making processes.

1.4	**Don’t believe your lying eyes. Seriously: AI-enabled deception erodes operational trust** AI is simultaneously allowing special operations forces to synthesize intelligence and coordinate missions at unprecedented speed while enabling adversaries to produce convincing deception at scale. The resulting contest will increasingly focus not just on collecting information, but on establishing which information can be trusted. (source) *Assessment:* Speaking at the Global SOF Foundation’s Indo-Pacific Irregular Warfare Symposium in Honolulu on August 19, U.S. Special Operations Command chief Admiral Frank Bradley warned that AI-generated deepfakes, synthetic voices, cloned faces, and fabricated identities are degrading confidence in digital information upon which modern military operations rely. Bradley told the audience of international special operators, industry representatives, and lawmakers that he had personally “been plagued by my own staff hijinks” involving AI-generated content convincing enough to fool colleagues. Again, according to Bradley, “if you weren't part of the inside crew, you probably couldn't tell the difference because of how capable AI is at creating deepfake content.” A U.S. military official working in counterintelligence and foreign-influence analysis put the challenge more starkly: “AI has made deception scalable,” turning what was once an expensive, technically demanding capability into one available to low-resourced actors. At the tactical level, manipulated intelligence or corrupted data could disrupt targeting, undermine command and control, or induce forces to act against fabricated threats. At the strategic level, uncertainty about the authenticity of information could make it harder for leaders to attribute hostile actions, build public and allied support, or generate the unity of effort that deterrence requires. More dangerously, convincing fabrications or corrupted intelligence introduced during a crisis could generate false indications of attack, complicate attribution, and push leaders toward escalation before the underlying information can be authenticated. The Symposium discussion revealed another dimension of the significant AI tension facing defence communities explored in the first story of this section on the impact of advanced AI model diffusion for cyber security. Militaries are becoming increasingly reliant on AI to construct the operational picture at the same time adversaries are using AI to corrupt it and the data on which these models operate. As Bradley summarized, “Information advantage leads to decision advantage”, but only when commanders can trust the information on which those decisions depend.

2. Robotics and Autonomous Systems

2.1	**The Thunder King, the Ghost Bat, and another approach to uncrewed tactical air** Two events highlighted the continued and rapid transition of Collaborative Combat Aircraft (CCA) from developmental concepts into an increasingly competitive global market that appears to be bifurcating into low-cost attritable designs and high-end alternatives. (source, source, source, and source) *Assessment:* During the Farnborough Airshow outside of London in July, both Boeing and BAE displayed concepts for CCA programs. BAE displayed the Brontanax (taken from ancient Greek and meaning “Thunder King”), its entry for the RAF’s Storm Fighter program to field a sovereign, autonomous CCA. The program is backed by £300 million in UK defence funding, and the system is intended to fly alongside the Typhoon in the short term and the Global Combat Air Programme (GCAP) in the 2030s. BAE is targeting 70–80 percent of a Typhoon's mission capability at 20–25 percent of the cost, betting several hundred million pounds of its own money on a program analysts value at over $3 billion. Boeing’s Ghost Bat—first developed by Boeing Australia—also appeared at Farnborough, arriving after having already crossed important operational thresholds. In December 2025 at Woomera, an MQ-28 became the first uncrewed aircraft to complete an autonomous air-to-air engagement, destroying a target drone with an AIM-120 AMRAAM after an E-7A Wedgetail operator retained "custodianship" and authorized the shot. In June 2026, it became the first CCA to fly in a multinational exercise, teaming with F-35s during Valiant Shield. During the show, Boeing representatives also rolled out a new concept for Ghost Bat production that includes more numerous, smaller, and dispersed factories building the systems with the aim of specific partner nations, producing the systems “to meet their own local needs [rather] than having one mega factory,” according to Glen Ferguson, MQ-28 global program director. Ferguson also emphasized the value this approach brings in a “supply chain denied environment.” By contrast, Saab is developing a different approach to CCAs that varies from the attritable, low-cost model. Unveiled 21 August at Malmen Air Base for the Swedish Air Force's centennial, the A3 is a tailless, stealthy, and supersonic design. It is intended as a "peer-capable complement" for electronic warfare, air-defence suppression, and precision strike rather than routine, expendable missions. The reveal of the A3 comes during a time when the Swedish government is evaluating ways of replacing its Gripen fleet in the 2040s, though Saab is not positioning the A3 as the replacement. As Peter Nilsson, head of Saab’s advanced programs unit, told journalists, the A3 is an “offer” to help move the Swedish Air Force “into the unmanned space” and complement the Gripen E in combat. The three programs suggest CCA competition is both urgent *and* divergent. Momentum for UASs capable of carrying out roles in conjunction with crewed fighter jets is growing. At the same time, multiple visions for what these aircraft could and should look like have emerged. Most seek to deliver affordable scale using less capable but also less expensive systems. Saab’s A3 offers another vision revolving around a more capable aircraft than their attritable counterparts but also one that is more complex and expensive.

Figure 1: Top: The Ghost Bat MQ-28 taxiing during Exercise Valiant Shield on June 21, 2026; Middle: A mock-up of the Brontanax displayed during the Farnborough Air Show; Bottom: The Saab supersonic, low-observable A3 collaborative combat aircraft concept. Sources: Senior Airman Adrien Tran/U.S. Air Force via Defense News; BAE Systems, and Saab, via Aviation Week

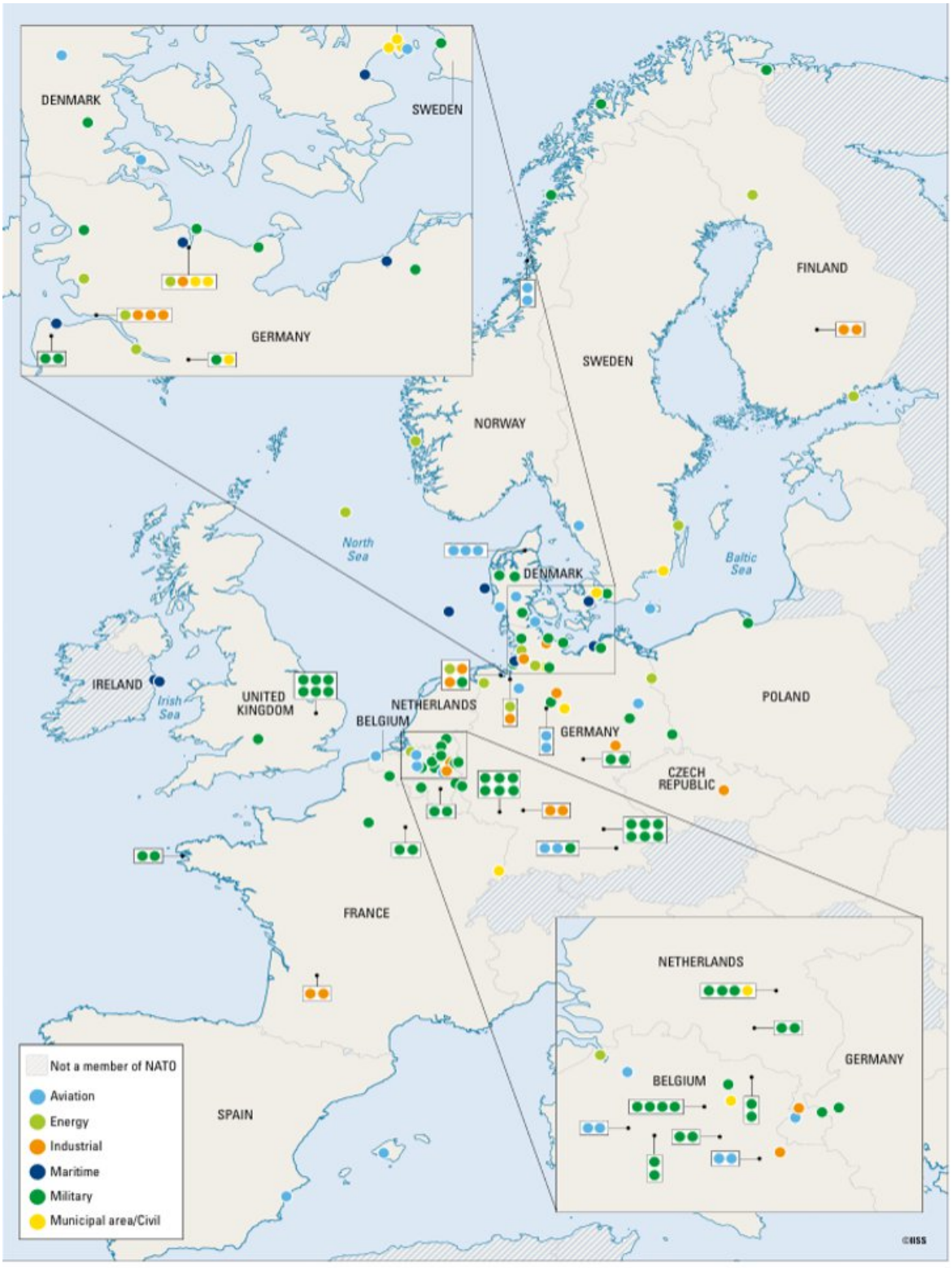
2.2	**South Korea selects its first operational multipurpose UGV** South Korea has selected Hanwha Aerospace's ARION-SMET over Hyundai Rotem's competing HR-Sherpa for the Republic of Korea Army's first operational multipurpose UGV program. The award marks an important transition from military robotics experimentation to serial production and fielding. (source) *Assessment:* The six-wheeled, all-electric ARION-SMET is designed as a modular support platform capable of transporting ammunition and equipment, conducting reconnaissance and surveillance, evacuating casualties, and supporting close combat. It can autonomously navigate off-road, follow soldiers or vehicles, and return to a designated location if communications are lost. The vehicle can carry up to 550 kilograms, travel approximately 100 kilometres on a single charge, and reach 43 kilometres per hour on paved roads. The system's remote-controlled weapon station uses AI-enabled object recognition and acoustic gunshot localization to cue toward a suspected shooter, but final engagement requires authorization from a human operator, an important practical example of the human control questions raised elsewhere in this volume. South Korea's Ministry of National Defense has been explicit that the program is meant to address shrinking troop numbers as much as any technology gaps. The active-duty force has fallen from roughly 560,000 in 2019 to about 450,000 today, even as the equipment load carried by individual soldiers has grown. The initial contract, worth approximately KRW 49.6 billion (about $33.5 million), covers a first batch of vehicles for fielding in 2027–2028. A follow-on award, potentially worth ten times as much, could come as early as 2029, depending on Army requirements. The vehicle supports South Korea's Army TIGER 4.0 modernization initiative, which seeks to build a more networked and autonomous ground force. While the system's capabilities are intriguing, the decision's significance rests primarily in the movement of an autonomous ground platform into routine force structure where its reliability, maintainability, doctrinal utility, and integration with soldiers will be tested at meaningful scale.

Figure 2: Hanwha's ARION-SMET multipurpose UGV. Source: Yonhap News

2.3	**Modularity reducing need for mission-specific uncrewed systems** A novel partnership between Ghostworks Marine, General Atomics, and Mercury Marine has unveiled Multirole Remote Logistics Node (MRLN), a remote-piloting and autonomy system that converts high-performance vessels into reconfigurable, uncrewed platforms for five missions: intelligence, surveillance, and reconnaissance (ISR); littoral resupply; mine countermeasures; communications relay; and combat logistics support. (source and source) *Assessment:* MRLN is a modular mission-systems layer deployable across Ghostworks' M-Hull and powercat designs, giving commanders human-in-the-loop command over systems mission to mission rather than needing a separate purpose-built boat for each task. The partnership behind MRLN is deliberately unconventional. • Ghostworks, a boutique composite shipyard based in Holland, Michigan, designed and built the vessel. • General Atomics Aeronautical Systems Inc. (GA-ASI), far better known for the MQ-9 Reaper, adapted autonomy and sensor software developed for remotely piloted aircraft to the maritime domain. • Mercury Marine, a brand more associated with recreational outboard engines than defence contracts, supplied the drive-by-wire propulsion and Command Gateway systems that let the vessel steer, throttle, and hold station while operating remotely. That an aircraft-autonomy specialist and an outboard-motor manufacturer are now co-engineering a naval logistics platform is itself a small data point on how porous the line between commercial and defence autonomy has become. The first installation is aboard *Minerva*, a 40-foot carbon-fibre M-Hull vessel capable of carrying 17,500 pounds while cruising at 30 knots and operating in Sea State 4. Human operators will retain full situational awareness and can assume direct control at any point even while the vessel runs autonomously. MRLN's mission-agnostic design can reduce costs of fielding uncrewed system fleets. Rather than having to procure separate uncrewed vessels for surveillance, logistics, mine warfare, and communications, commanders can reconfigure a common platform in the field, potentially reducing procurement and sustainment burdens while letting autonomous fleets adapt faster to operational needs. The concept is especially relevant to distributed maritime operations in the Indo-Pacific, where forces will need persistent sensing, resilient communications, and repeated resupply across widely dispersed and contested locations.

2.4	**World Cup drone incursions expose a changing infrastructure threat** By the close of the FIFA World Cup tournament in the United States over the summer, U.S. federal authorities had detected nearly 1,600 drones operating in restricted airspace around tournament venues and seized more than 700 across all 11 U.S. host cities. The FBI and Department of Homeland Security (DHS) deployed specialized counter-UAS teams to detect, track, identify, and intercept the aircraft, although most of the government's mitigation methods remain classified. (source, source, and source) *Assessment:* While the 1,600 drones detected and 700 seized are both significant numbers, another important number that relays the scale of the challenge of monitoring the drone threat, especially during large events, is the gap between the drones that were detected and those that were confiscated. Authorities had to assess a far larger volume of activity than ultimately required confiscation or mitigation, complicating the counter-drone task during the event. FBI Director Kash Patel described the operation's size by comparing it to running "78 Super Bowls in 38 days," and the tournament ultimately recorded no significant security incidents. Of course, most World Cup violations were careless or recreational. However, at an operational level, intent cannot be assumed at the moment of detection. Every unidentified drone must be detected, classified, tracked, and, if necessary, defeated before authorities know whether it is filming a match or carrying a dangerous payload. Large numbers of benign violations can saturate sensors and response teams, obscure deliberate reconnaissance, or provide cover for a coordinated attack. A second challenge for governments and national security communities throughout the world reflected by the U.S. counter-drone operations is the difficulty in sustaining successful infrastructure protection operations outside of special event protection. Counter-drone operations during the FIFA World Cup worked because they were supported by approximately $625 million in federal funding and because relevant agencies fielded roughly 60 state and local officers certified in electronic mitigation, layered under a federal detection and response architecture sustained continuously for more than five weeks. As commercial drones become more capable and available and many governments seek to use drones for grey-zone surveillance and coercive activities (as discussed in the story below), the threat to civilian, government, and military critical infrastructure has become more pronounced and difficult to detect and track. Scaled and organized responses can help mitigate these risks to infrastructure during times of heightened tension or special events. However, effective defence outside of these occasions will require persistent sensing, rapid identification, clear legal authorities, coordination across federal and local agencies, and systems and personnel capable of distinguishing genuine threats from a large volume of everyday drone activity without exhausting the response capacity needed to confront a real attack.

2.5	**Reconnaissance by battle: Russia testing and learning about Europe's defences through UAS operations** A report from the International Institute for Strategic Studies (IISS), co-authored with the Hanns Seidel Foundation, assesses that Russia likely conducted a coordinated UAS campaign across Europe between August 2024 and February 2026 designed to surveil, disrupt, and test European capabilities. (source) *Assessment:* The study identified 144 incidents across 13 European countries, 48 percent over military bases, 26 percent over critical infrastructure, and 18 percent over civilian airports, including incursions near NATO nuclear-sharing bases believed to host American B61-12 gravity bombs and France's ballistic missile submarine facility at Île Longue. According to IISS, the uncrewed systems campaign represents an aerial extension of Russia's wider unconventional warfare against Europe. Rather than attacking targets directly, low-cost and difficult-to-attribute UASs were used to collect intelligence, disrupt civilian activity, and test European responses through repeated airspace violations below the threshold likely to trigger collective retaliation. Germany recorded the most incidents, with 58, followed by Belgium with 25 and Denmark with 16. Drones appeared over Ramstein Air Base and RAF Lakenheath, among other facilities. The report describes the approach as an airborne version of the Soviet-era concept of "reconnaissance by battle": Even if a drone is detected or defeated, Russia can still gain intelligence on response times, radar coverage, and rules of engagement. A September 2025 incident illustrates the cost of that ambiguity alone. Drone sightings forced Copenhagen Airport to close for four hours, disrupting approximately 190 flights, without a single Russian asset ever being definitively identified. The maritime dimension is especially concerning. The report assesses that Russian-linked shadow-fleet tankers likely served as mobile launch and recovery platforms. One cited case is the *Boracay*, a Benin-flagged, EU-sanctioned tanker boarded by French forces off Saint-Nazaire in late September 2025 after it was identified as one of several Russian-linked vessels operating near Denmark during that month's drone incursions. Although no direct connection to the drones was established, the vessel's opaque registration, shifting identities, and manipulation of tracking data illustrated precisely the attribution problems such platforms create. Launching from international waters allows UASs to approach targets without crossing monitored land borders while exploiting opaque ownership and manipulated vessel-tracking data. The authors assess that Europe's counter-UAS architecture remains poorly matched to this activity, stating that "detection is uneven, legal authorities are fragmented, response options are often disproportionate, and attribution remains too slow to support timely deterrence." The campaign's most important achievement may have been exposing the gap between capability and authority as governments often had systems capable of engaging suspicious UAVs but lacked the clearance or confidence in attribution to use them. The report also asserts that the European Drone Defence Initiative (EDDI), which aims to build a continent-wide, 360-degree counter-drone architecture and achieve initial operational capability by the end of 2026 lacks the agility and doctrinal coherence required to deliver scalable results in part because it "will only target the UAV once it enters European airspace – there is no mandate over the vessel that launched it."



UAV = uninhabited aerial vehicle
Note: Sightings of UAVs related to the war in Ukraine are not shown.
Sources: IISS analysis; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com

Figure 3: Selected reported UAV sightings in Europe by location and site, August 2024–February 2026. Source: Russia's UAV Campaign Over Europe

4. Manufacturing and Industry

3.1	**German-Ukrainian drone production creates a new industrial model** Germany and Ukraine are moving beyond the traditional military-assistance model toward jointly financed and integrated weapons production. Germany is financing production of thousands of systems annually for Ukraine, with designs also intended to satisfy future German and allied requirements. (source and source) *Assessment:* The most prominent examples of this new approach are Anubis and Seth-X, two AI-enabled strike drones being developed through a joint venture between Ukrainian manufacturer Airlogix and Auterion, a U.S.-based autonomy-software company with European headquarters in Munich. Anubis is a medium-range platform intended to strike personnel, armoured vehicles, and tactical or strategic targets deeper behind Russian lines. Seth-X is a smaller system optimized for shorter-range attacks against troops, light armour, logistics, and transport. Both incorporate Auterion's Skynode flight computer and Nemyx autonomy software, intended to support navigation, target identification, and terminal guidance in environments where electronic warfare disrupts conventional communications and satellite navigation. A *Medium* article describes the development as the end of the "donation era" and the beginning of an "age of the Joint Strike." The underlying industrial point is valid. Germany is no longer simply purchasing finished weapons and transferring them but helping build an enduring cross-border production ecosystem. The joint venture was announced from the stage at the Munich Security Conference in February 2026 by Auterion CEO Lorenz Meier and Airlogix CEO Vitalii Kolesnichenko, and the first production contract was signed in Berlin in April with Chancellor Friedrich Merz and President Zelensky present. It formed part of a broader package of German-Ukrainian production agreements under the "Build with Ukraine" initiative, including a separate Helsing–Culver Aerospace deep-strike partnership, suggesting this is becoming a template for industrial partnership rather than a one-off. According to the *Medium* article, the development would be of concern to Russia because it will enable a weapons production capability that can survive changes in individual aid packages and generate thousands of increasingly autonomous weapons with the added benefit of being designed from the outset to meet German Bundeswehr procurement requirements as well. The strategic shift is from transferring finite inventories to creating renewable, distributed, and combat-informed manufacturing capacity.

Figure 4: Top: Ukrainian President Volodymyr Zelenskyy and German Chancellor Friedrich Merz inspect the Anubis long-range strike drone. Image: Auterion; Bottom: A close-up view of the Seth-X strike drone, showcasing its four-wing criss-cross design and internal structure. Image: Airlogix

3.2	**Tokyo drift: Japan considers state ownership to secure defence production** Japan's government is weighing a shift to a government-owned, contractor-operated (GOCO) model for defence production. Under the model, the state would finance and own selected munitions and equipment factories while private companies handled daily operations. (source) *Assessment:* According to the *Japan Times,* the proposal has been included in a draft of the government's annual Basic Policy on Economic and Fiscal Management and Reform and reflects growing recognition that defence-industrial capacity cannot always be sustained through conventional commercial incentives. Munitions plants require substantial upfront investment but receive inconsistent peacetime orders, giving private firms limited reason to maintain excess capacity that matters only in a crisis. This problem is especially acute in Japan, where production has long concentrated in a handful of firms such as Mitsubishi Heavy Industries and Japan Steel Works. State ownership would shift that risk onto the government while retaining private-sector manufacturing expertise, giving Tokyo greater control over facilities whose interruption would create serious operational vulnerabilities. Japan is not seeking to fully nationalize industry. Instead, the proposal, which would require revising Japan's defence production and technology infrastructure law, concerns ownership of selected factories, not the companies themselves. The model mirrors the GOCO arrangement the U.S. Army has used since World War II at plants like Lake City, and one Australia is now building with Thales and Nioa. However, adopting it would mark a significant break from Japan's postwar reliance on purely private, market-driven defence manufacturing. The initiative forms part of a broader transformation of Japan's defence-industrial policy, alongside eased arms-export restrictions, encouragement for financial institutions to invest in defence firms, and expanded international and academic research cooperation.

3.3	**Supply-chain shadows: Foreign technology creates vulnerabilities in both directions** Two reports during the reporting period demonstrate how opaque and interconnected technology supply chains can introduce adversary-controlled components into Western military systems while allowing potential adversaries to acquire Western hardware and AI capabilities for strategically important applications. (source and source) *Assessment:* *BBC* reporting from 10 August, reveals that a routine UK Ministry of Defence cyber assessment discovered 20 Royal Navy K3 Scout uncrewed surface vessels (USVs) built by Kraken Technology Group and used by Royal Marines and special forces contained Chinese-made cameras transmitting "heartbeat" signals to a Chinese IP address. To be sure, the MoD found "no evidence of MoD data or systems being accessed, compromised, or transmitted externally" and the MoD removed the cameras' internet connectivity. Notably, Kraken maintains the cameras were certified as being compliant with the strict U.S. National Defense Authorization Act (NDAA) standards required to sell to the U.S. DoD, underscoring that formal certification did not identify the issue. A *Reuters* report from 31 July shows that supply chain security broadens the challenge beyond physical components. A *Reuters* review of more than 80 Chinese academic papers and patents, conducted with the Jamestown Foundation, found PLA-linked institutions using outputs from OpenAI and Anthropic models to train specialized domestic systems through "model distillation." Researchers at the PLA's National University of Defense Technology distilled a U.S. image-processing model to run navigation and targeting analysis directly on drones; the Academy of Military Sciences built a target recognition system for simulated maritime operations involving drones, ships, and submarines; and PLA Unit 96941, a Beijing-based military intelligence and cyber unit, used GPT-3.5 to summarize military source code for training a domestic model that runs entirely on internal networks. These cases demonstrate that supply-chain security now encompasses hardware, firmware, software, data, and AI models. Certification and export controls remain necessary but are insufficient when NDAA-compliant components still contain unrecognized communications pathways and commercially accessible model outputs can transfer advanced capabilities without a conventional sale. Effective protection requires continuous technical testing, component-level provenance, intelligence-informed customer screening, and a clearer understanding of how ostensibly civilian technologies can be recombined into military advantage.

5. Connectivity

4.1	**Beating the system: China places electronic warfare at the centre of modern conflict** *Armada International*'s August 2026 electronic-warfare special edition examines how the People's Liberation Army (PLA) integrates electronic attack, cyber operations, deception, intelligence collection, and precision strike within a doctrine known as "systems destruction warfare." This approach is aimed not at any one weapon system, but at the networks connecting them. (source) *Assessment:* The PLA doctrine of systems warfare emerged partly from the PLA's study of U.S.-led operations since the 1991 Gulf War, in which Chinese strategists concluded that modern military advantage depends less on individual platforms than on the sensors, communications networks, command structures, and data flows connecting them. An adversary's aircraft, ships, missiles, and ground forces may remain physically intact yet become operationally ineffective if their ability to sense, communicate, coordinate, and decide is disrupted. Tate Nurkin, founder of OTH Intelligence Group (the author of this Deftech Scan report who was interviewed for the *Armada International* report), described the logic: "By degrading the networking system, you don't have to worry about the technological sophistication of an adversary's platforms." At the operational level, the doctrine targets command-and-control nodes, kill chains, ISR systems, communications networks, radars, and satellite-enabled navigation and timing, reinforced by precision kinetic strikes against the most important nodes. Systems such as the J-16D electronic-warfare aircraft, first displayed publicly at Zhuhai in 2021, provide a visible example of the specialized hardware being developed to execute this approach. At the tactical level, PLA combined-arms brigades field organic EW units tasked with locating and jamming communications, radars, drones, and precision-guided weapons. This systems-oriented approach is complemented in the cognitive domain by China's long-standing "Three Warfares" framework that emphasizes public opinion, psychological, and legal warfare to shape perceptions and decision-making rather than disable hardware. The *Armada* report also highlights the close integration of China's military, state-owned defence-electronics companies, universities, and broader scientific community. This ecosystem supports rapid development across EW, artificial intelligence, quantum sensing, and related fields. Of course, uncertainty remains about the maturity and real-world effectiveness of specific Chinese systems, though dismissing public claims entirely as propaganda should be avoided, and analysts should "take China's overall scientific progress seriously." The PLA's actual capabilities remain incompletely understood, but between the doctrine and the hardware described in the *Armada* article as well as additional organizational reform, the PLA's intentions are more transparent. So, too, is the broader theme that future wars will be won as much by eroding and degrading the systems that allow an adversary to fight as by destroying its individual weapons.

4.2	**Switching platforms, shifting alignment: Pakistan's Army moves from WhatsApp to WeChat** The Pakistan Army has reportedly instructed military and administrative personnel to phase out Meta-owned WhatsApp for official communications and transition to Tencent's WeChat. The change was attributed to concerns about surveillance, interception, and data breaches on Western platforms, although Pakistan's Inter-Services Public Relations has not publicly confirmed the directive. (source) *Assessment:* The reported transition reflects the expanding technological dimension of the China–Pakistan strategic relationship. Cooperation that has long included combat aircraft, warships, missiles, and other military hardware may now be extending into digital communications infrastructure and common operating practices. Moving to WeChat could facilitate coordination with Chinese counterparts during exercises and joint activities. It also signals declining Pakistani trust in Western technology providers and a broader tendency among governments to align their digital ecosystems with their principal security partners. However, replacing one foreign-owned commercial platform with another does not resolve the underlying communications-security problem. It simply changes which external company, and which foreign legal and regulatory system, controls the platform, data architecture, and metadata. Notably, the Pakistani government appears to recognize the same underlying problem and has taken initial efforts to mitigate its reliance on foreign technology companies. Pakistan's National Information Technology Board is in the process of developing "Beep," a domestically hosted, WeChat-inspired messaging app intended for government use, with a phased rollout beginning in federal ministries. That Islamabad chose a foreign platform for its military's most urgent needs while a sovereign alternative was still maturing suggests operational alignment with Beijing outweighed, at least for now, the data-sovereignty logic driving the domestic "Beep" project. In addition to the geopolitical relevance, the decision also highlights the blurring of lines between seemingly ordinary commercial applications and first-order national security concerns. Communications platforms are becoming instruments of geopolitical alignment, but militaries relying on them remain exposed to foreign ownership, uncertain data governance, and limited sovereign control over essential information infrastructure.

4.3	**No sanctuary: Commercial companies targeted in cyber and kinetic attacks designed to undermine economies and affect commercial-military ties** A Russian cyberattack against Jaguar Land Rover in the UK and Ukrainian drone strikes against Wildberries storage and distribution warehouses illustrate how conflict is expanding beyond traditional military targets into the commercial networks that generate economic output, sustain military operations, and structure everyday life. (source and source) *Assessment:* *New York Times* reporting from 26 June revealed the extent of the damage and lack of definitive attribution of the 2025 cyberattack against Jaguar Land Rover in the UK. The attack began on 31 August 2025 and shut down production for approximately five weeks at plants in the UK and abroad. The FBI, UK National Crime Agency, and Google's Mandiant unit reportedly traced the operation to Russian hackers rather than the "loose collective" that initially claimed responsibility on Telegram. Investigators also discovered that at least two other intruders had previously breached JLR's network, suggesting its defences had been porous for some time. The attack cost Jaguar approximately $350 million directly and produced an estimated $2.5 billion loss across the British economy, affecting more than 5,000 organizations connected to the Jaguar Land Rover supply chain. This made it the most financially damaging cyberattack in UK history. Notably, no ransom was ever demanded. As former UK armed forces minister Al Carns observed: "There was no ransom demand... They just wanted to see if they could do it." This absence of a ransom demand raises the possibility that the operation was intended, at least in part, to demonstrate the capacity to generate cascading economic effects on the UK economy through targeting one deeply integrated manufacturer without physically attacking a factory. Ukraine's strikes against Wildberries, Russia's largest online retailer, reflect a more overt and kinetic version of the same approach. Since the campaign began in mid-July 2026, Ukrainian drones have repeatedly struck the company's facilities, destroying its largest logistics hub at Koledino and disabling at least seven of its ten largest distribution centres, according to Ukraine's Defence Ministry. Kyiv argues that the warehouses distribute drone components, fibre-optic cable, body armour, and other dual-use equipment to Russian forces. The commander of Ukraine's 429th Separate Unmanned Systems Brigade, Yurii Fedorenko, said the resulting shortages forced Russian units to restrict their use of cameras, propellers, controllers, and batteries. However, Wildberries is better known for being deeply embedded in Russian civilian life. Much of the destroyed warehouse space and inventory was reportedly uninsured, leaving small sellers who stored goods there exposed to substantial losses. The campaign has since expanded to competitor Ozon, first struck on 22 August. Attacking these distribution networks therefore disrupts military logistics, commercial activity, and public perceptions of security simultaneously. While the mode of attack varies in these cases, they reveal the erosion of the distinction between military, economic, and social infrastructure. Modern forces depend on civilian manufacturers, digital platforms, commercial logistics providers, and distributed suppliers. This integration creates resilience and scale, but it also converts ordinary companies into potential vectors of strategic pressure.

4.4	**New Mexico tragedy highlights growing civil-aviation risk in U.S. and elsewhere to increasingly sophisticated jamming and spoofing** The U.S. National Transportation Safety Board (NTSB) is investigating whether military GPS jamming contributed to the May 14 crash of a Beechcraft King Air C90 medevac aircraft in New Mexico that killed four. While this crash was an accident, it reignited debate over civil aviation vulnerability to electronic warfare and reinforces the theme of the erosion of trust in mission critical data in the age of intensifying cyber and electronic warfare. (source and source) *Assessment:* The aircraft was approaching the resort town of Ruidoso, about 70 miles from Roswell, NM, to collect a patient when its pilots reported losing GPS reception. An air-traffic supervisor asked personnel conducting a jamming exercise at White Sands Missile Range to suspend operations but later authorized their resumption. Five minutes afterward, the aircraft struck the Capitan Mountains, killing both pilots and two nurses. Three other aircraft reported GPS disruption that night, although the NTSB has not determined the crash's probable cause. An *Aviation Week* podcast uses the incident to highlight the risks associated with civil aviation's growing exposure not just to accidental GNSS interference but malicious attempts at jamming and, especially, spoofing, which feeds aircraft convincing but false position or timing data. The effects of spoofing can propagate beyond navigation displays into flight-management systems, autopilots, terrain warnings, and other interconnected functions. While pilots can cross-check GNSS feeds against inertial systems, ground-based navigation aids, and air-traffic-control radar when jammed or spoofed, these fallbacks do not resolve the fundamental policy and technological gap between the sophistication and urgency of the threat and the approach civil aviation agencies in the United States are taking toward mitigating this threat. Military aircraft increasingly employ resilient antennas and multiple navigation signals, while many civilian aircraft remain heavily dependent on one GPS frequency. Wider adoption of the more robust GPS L5 signal across civil aviation has stalled and controlled-reception pattern antennas that can suppress interference face Federal Aviation Administration (FAA)cost and certification barriers as well as additional U.S. DoD barriers, which has until recently sought to control the proliferation of advanced anti-jamming and spoofing technologies. The deeper challenge is institutional. Civil aviation's deliberately cautious certification system is designed to prevent unsafe technologies from entering service. However, it is poorly adapted to counter threats evolving faster than equipment can be approved and installed. Growing military jamming exercises and persistent interference around conflict zones make navigation disruption a systemic civil-military risk, requiring better real-time coordination, accelerated certification of proven protections, improved crew training, and layered alternatives to satellite navigation.

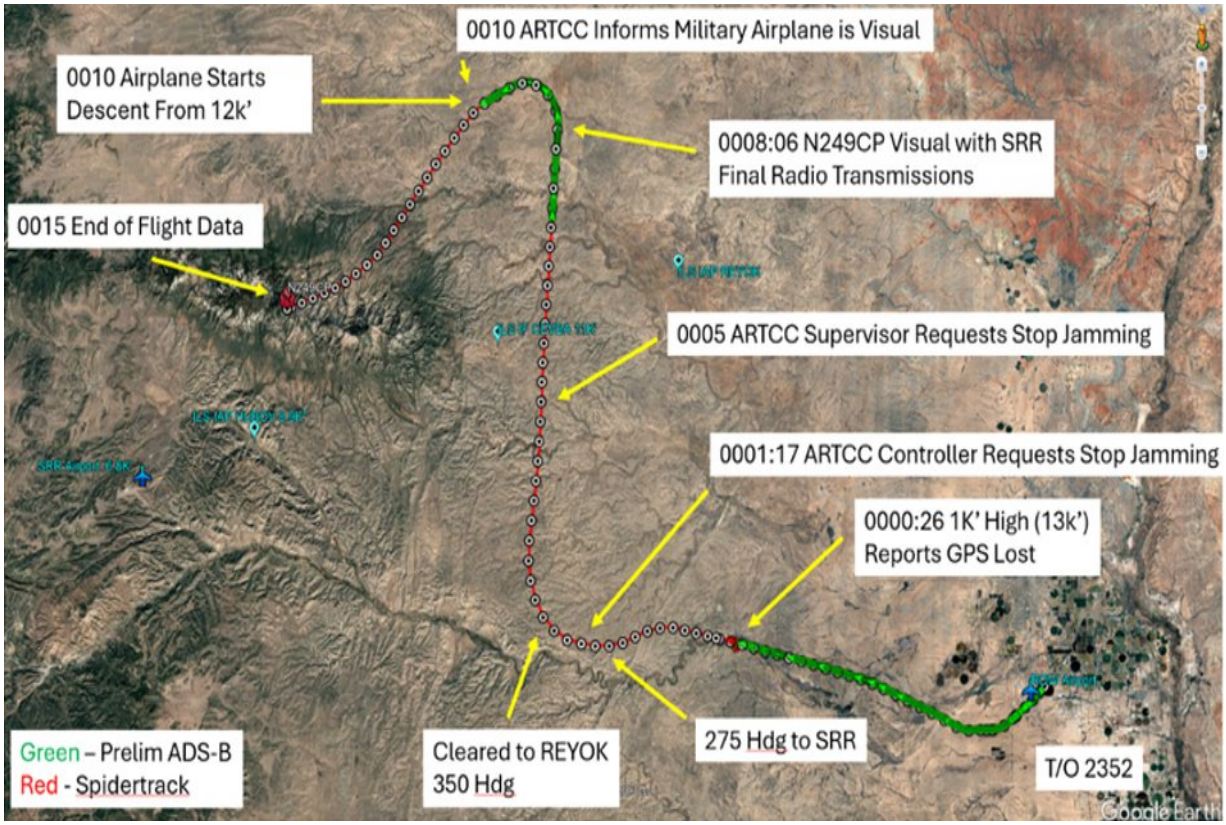


Figure 5: A figure published by the National Transportation Safety Board shows the flight path of a Beechcraft King Air C90 medevac plane that crashed into the Capitan Mountains on May 14, 2026. (National Transportation Safety Board)

6. Platforms and Weapons Systems

5.1	**Scaling up: India is developing a light-weight missile for mass drone strikes while France continues to scale its drone production through partnerships with automakers** India's Defence Research and Development Organisation (DRDO) is developing a lightweight air-to-ground missile intended to be launched from UASs against high-priority targets. The development reflects a growing trend toward using and manufacturing smaller, lower cost munitions and drones at scale. (source, source, and source) *Assessment:* India is developing an unusually lightweight precision-guided missile designed to arm smaller uncrewed aircraft, while France is mobilizing civilian manufacturing capacity to increase drone and loitering-munition production. Together, the initiatives demonstrate how militaries are seeking greater combat mass not only by buying more platforms, but by reducing the size and cost of individual systems and adapting commercial production methods to manufacture them at scale. India's missile reportedly weighs approximately 10–15 kilograms and carries a roughly 2-kilogram warhead, allowing relatively small drones to engage vehicles, personnel, and other tactical targets. Modular warhead options and navigation designed to function in jammed environments would expand its utility across different missions. The weapon could give inexpensive UAVs a precision-strike capability previously associated with larger, costlier aircraft, while allowing a single platform to carry multiple rounds. France is approaching the same mass problem from the industrial side. Renault and Thales plan to manufacture as many as 1,000 Toutatis loitering munitions per month from 2027, up from Thales's current output of roughly 100 annually. Renault's automotive expertise—including injection moulding, simplified designs, and reduced parts counts—is intended to lower costs and accelerate production. Alongside other partnerships involving Renault, Delair, Schaeffler, Forvia, and French defence companies, announced production targets could approach 60,000 systems annually. Both developments reflect a broader redefinition of military scale. Smaller weapons can distribute precision effects across more platforms, while simplified designs can open production to civilian manufacturers operating at commercial volumes. The result is not merely more drones and munitions, but a more resilient model of combat power: numerous, replaceable systems carrying appropriately sized effects and supported by production networks capable of regenerating losses. The principal challenge going forward will be matching impressive theoretical production capacity with sustained orders, secure component supplies, and operational concepts capable of employing mass effectively.


deftech.ch