DEFENCE TECHNOLOGY TRENDS

China is increasingly **prioritising science and technology (S&T) as a central pillar of national strategy,** accelerating its push for technological self-reliance. Its upcoming five-year plan channels major investment into AI, quantum, 6G, brain–computer interfaces, and robotics, sectors critical to both economic competitiveness and military modernisation. This integrated approach is reflected in a 7% increase in defence spending for 2026, bringing the official budget to roughly $277 billion, with significant resources directed toward AI-enabled systems, advanced computing, and robotics.

As highlighted by CEPA, for **Western countries, technological leadership is now a coalition game, not a national one.** China is acting as a coherent, state-driven system, aligning industrial policy, innovation, and military development. By contrast, the West risks acting as fragmented competitors despite deep interdependence across supply chains, semiconductors, and research ecosystems. **NATO countries must collectively treat R&D as a core warfare enabler**, with increased investment and common standards to strengthen innovation and interoperability across allies. Maintaining a technological edge will depend on tighter coordination of allied industrial and scientific capabilities, particularly in securing critical supply chains.

ACPT Wire | Reuters | Foreign Affairs | CEPA

NATO COUNTRIES AND PARTNERS

Operation Epic Fury in Iran illustrates **the growing integration of AI into modern military operations**, where it is used to **accelerate targeting processes and fuse intelligence across domains**. The involvement of major technology companies such as Microsoft, Google, and Amazon highlights how commercial technologies are now embedded directly into warfare, blurring the boundary between civilian industry and military activity. In parallel, tools developed by Palantir Technologies and Anthropic (Claude) are supporting intelligence analysis, target identification, and operational planning for U.S. and Israeli forces. **AI systems are reportedly processing around 1,000 potential targets per day**, **compressing decision cycles from days to seconds**; however, as of now, human operators retain final authority over lethal decisions.

AI Magazine | CBS News | Defense Scoop | CEPA

The Pentagon is expanding its use of AI in two major areas: cyber warfare and internal operations. It is developing AI-powered tools to automatically identify and map vulnerabilities in Chinese infrastructure, such as power grids and sensitive networks, so potential targets can be incorporated into U.S. war planning at far greater scale than human hackers alone. At the same time, the DoD is rolling out AI agents powered by Google's Gemini across its three-million-person workforce to automate routine administrative work on unclassified networks, including summarising notes, drafting budgets, and assisting with large-scale military planning.

Financial Times | Bloomberg

The U.S. Air Force's Collaborative Combat Aircraft (CCA) programme is increasingly centred on AI autonomy software that acts as the "pilot" for unmanned fighter drones operating alongside human pilots. Two competing AI systems are being developed: **Sidekick**, provided by Collins Aerospace, and **Hivemind**, provided by Shield AI. These systems are designed to be platform-agnostic, meaning they can control different aircraft types rather than being tied to a specific drone.

Air&Space Forces Magazine

The **U.S. DoD is developing AI-driven cognitive warfare capabilities** to influence how adversaries perceive and act by shaping narratives across digital environments. The BIAO programme combines tools to detect adversary-generated disinformation with systems that generate and test multimodal influence content, moving beyond general models like ChatGPT or Google Gemini. Its central aim is to conduct influence operations at "machine speed," enabling rapid deployment, evaluation, and refinement of messaging in real time.

National DEFENSE

Ukraine has launched a new programme to let trusted foreign partners and defence companies train AI systems on real combat data from the war. Ukraine says its vast, continuously updated collection of labelled combat imagery gives partners a rare chance to improve AI models using real-world battlefield conditions. In return, Ukraine expects faster co-development of advanced autonomous capabilities for use on its own front lines.

Defense News

The **Gulf conflict** marks a **shift in warfare,** with **data centres and tech infrastructure emerging as direct military targets alongside traditional assets**. Iranian strikes on cloud facilities and threats against major U.S. tech firms highlight how critical private-sector digital infrastructure has become to both economic stability and military operations. This reflects a broader trend seen in Ukraine, where close cooperation between governments and technology companies has enabled data-driven, AI-enabled warfare, effectively placing tech firms on the front lines. As a result, the U.S. and NATO must strengthen protective measures to safeguard these assets.

CSIS

The **U.S. Army's 2nd Cavalry Regiment in Europe is testing 17 unmanned ground vehicles (UGVs)** as part of the xTech Edge Strike Ground competition. The systems could support missions such as logistics resupply, casualty evacuation, and explosive delivery against enemy positions. One of the most promising uses is battlefield breaching, to clear obstacles without exposing troops. **In the maritime domain,** The U.S. Navy and the Pentagon's DIU selected **Anduril** for the **development of a new extra-large unmanned underwater vessel** for deep, long-endurance missions. Its Dive-XL platform can travel more than 2,000 nautical miles, carry multiple payload modules, and function as a mothership for surveillance or strike operations using smaller underwater drones. The **U.S. Navy is also shifting to a faster, marketplace-style system** to acquire medium unmanned surface vessels (MUSVs). Similarly, **in the air domain**, The U.S. Army is revolutionizing drone acquisition with the launch of an **"Uncrewed Aircraft System Marketplace,"** an open solicitation that will remain active "in perpetuity" to allow for rapid commercial tech integration.

Breaking Defense | Defense News | Defense Scoop |Defense News | Defense Scoop

Under Operation Epic Fury, the U.S. military conducted the first combat use of the **LUCAS one-way attack drone**, a $35,000 system reverse-engineered from the Iranian Shahed-136. At the same time, the U.S. plans to deploy in the region the **Merops counter-drone system**, which uses AI-guided interceptor drones to detect and destroy hostile drones, even in jammed environments, offering a cheaper alternative to using costly missile interceptors against low-cost threats.

Military Times | Business Insider | Defense News

Ukraine is increasingly relying on low-cost interceptor drones, costing around $3,000–$5,000 per unit, as a central component of its air defence against Russian aerial attacks. These drones now account for roughly one-third of all Russian aerial targets destroyed nationwide and more than 70% of Iranian-designed Shahed drone interceptions over Kyiv. Ukraine has rapidly expanded **interceptor production to around 100,000 units in 2025**, delivering thousands per day to frontline units. As highlighted by the Atlantic Council, this surge reflects the rapid growth of Ukraine's defence technology sector and its innovative approach to drone warfare, which is increasingly shaping modern battlefield practices. NATO Allies are increasingly leveraging Ukraine's battlefield experience, **while Kyiv has also deployed 228 drone specialists to five Middle Eastern countries to support efforts in countering Iranian drone threats**.

Defence News | Atlantic Council | War On The Rocks | Defense News

The **Defense Innovation Unit** successfully executed the Cassowary Vex suborbital hypersonic test, demonstrating a manoeuvrable platform capable of sustained flight above Mach 5. Conducted under the HyCAT programme, the mission helps **relieve a national bottleneck in hypersonic testing** by providing affordable, high-cadence flight opportunities critical for accelerating more than 70 U.S. defence hypersonic initiatives. The **demonstrator's airframe was produced using additive manufacturing**, highlighting how 3D printing can rapidly produce hypersonic test vehicles and expand testing capacity.

Defence Innovation Unit

The Pentagon has raised the Golden Dome missile defence estimate to $185 billion, largely to accelerate space-based systems designed to track fast, manoeuvrable hypersonic threats, including the Hypersonic and Ballistic Tracking Space Sensor (HBTSS) and enhanced data networks. Separately, the **U.S. Space Force has awarded BAE Systems a $1.2 billion contract to build ten medium-Earth-orbit infrared satellites for hypersonic detection** as part of a broader multi-orbit sensing architecture. This programme has passed preliminary design review and reflects parallel efforts to strengthen global hypersonic tracking.

Air & Space Forces Magazine | Space News

Quantum technology enables new computing, sensing, and communication capabilities that could solve problems beyond the reach of classical systems. Its impact may soon be felt across **five key areas of everyday life, with clear military applications:** faster discovery of medicines and advanced materials, ultra-precise sensors for navigation and environmental monitoring, improved optimisation in logistics and finance, quantum-secure communications, and more powerful AI. However, these breakthroughs will likely emerge through **hybrid systems** that combine classical supercomputers with specialised quantum processors rather than replacing existing computing architectures. While the U.S. leads in both classical supercomputing and quantum research, Europe and Japan are moving faster to deploy integrated quantum-supercomputing infrastructure.

RAND | CSIS

The **Trump administration** has elevated **blockchain security and quantum-related risks to top national policy priorities** within its latest cybersecurity strategy. New measures, including an executive order, aim to strengthen federal systems through post-quantum cryptography, zero-trust architecture, and more resilient digital infrastructure. The strategy also highlights securing cryptocurrencies and blockchain technologies, while promoting quantum-safe solutions and the development of secure quantum computing capabilities.

BH News | Cyber Strategy for America

U.S. space forces played a foundational role in the opening phase of Operation Epic Fury by delivering "non-kinetic effects" that degraded Iran's ability to observe, communicate, and coordinate before conventional strikes began. Pentagon leaders have said that space and cyber operations were the "first movers" and the "backbone" of the campaign, disrupting Iranian sensor and communications networks and leaving Tehran with diminished situational awareness prior to the kinetic assault on over 1,000 targets in the first 24 hours. By blinding and disorienting Iranian C2 from orbit and across the electromagnetic domain, Space Command's effects helped set the conditions for follow-on air, missile, and strike operations to proceed with greater effectiveness.

Air&Space Forces Magazine | National Defense Magazine

Anduril announced plans to acquire ExoAnalytic Solutions, a move that will significantly expand its space workforce and sensing capabilities. ExoAnalytic operates a global network of more than 400 telescopes. By integrating these sensing assets with its AI technologies, **Anduril aims to improve how space-based data is collected, processed, and analysed to generate actionable intelligence.** The combined capabilities will enable faster detection, tracking, and analysis of objects and activity in orbit, enhancing situational awareness for defence and national security operations. In parallel, **Anduril Industries and Palantir Technologies have been identified as key developers of the software operating system for the "Golden Dome"** antimissile shield. Notably, traditional defence contractors such as Lockheed Martin and Northrop Grumman are participating as subcontractors within this consortium.

Air&Space Defense Magazine | Wall Street Journal

The **Pentagon's counter-drone task force recently conducted a high-energy laser test** with the Federal Aviation Administration, reflecting growing concern over frequent drone incursions, particularly along the U.S.–Mexico border, and the military's priority on developing counter-drone capabilities. **Laser-based directed energy weapons (DEW) in the U.S. have moved beyond laboratory research** into early operational deployment and advanced prototyping, with vehicle- and ship-mounted systems demonstrating effectiveness against drones and other short-range aerial threats within layered air-defence architectures. **Amid the current high-intensity conflict involving Iran, the Pentagon has further underscored the economic advantage of DEW**: a Patriot PAC-3 interceptor can cost about $3.7 million per missile, Iranian Shahed drones roughly $20,000–$50,000, while a laser shot may cost about $3.50. Despite this clear cost asymmetry, wider adoption remains constrained by engineering challenges that continue to limit scalability.

Air&Space Forces Magazine | Defense News | Defence Science Review | National Defense

Israeli **Elbit Systems** is developing **high-power laser weapons for installation on fighter jets and helicopters,** though timelines and technical specifics remain undisclosed. Israel's existing Iron Beam ground-based laser system is effective and low-cost but constrained by weather and atmospheric conditions. Moving laser capabilities airborne is expected to extend range, improve effectiveness, and enable earlier interception. The technology, now at an advanced engineering stage, could represent a major shift in countering swarms and support offensive operations.

Defense News

STRATEGIC COMPETITORS

China is executing a comprehensive, **whole-of-force transformation built around AI as it advances into the "intelligentization" phase of modernisation**. AI is being embedded across every major warfighting domain, powering autonomous vehicles, drone swarms, satellite-targeting tools, predictive logistics systems, and advanced decision-support platforms. Beyond hardware, the **PLA is integrating AI into cognitive and information warfare**, including systems designed to analyse global data flows, shape perceptions, and influence adversaries' decision-making. At the same time, **U.S. export controls on advanced semiconductors are accelerating China's push for technological self-reliance**, paradoxically helping China to achieve what earlier Chinese industrial policies could not: driving large-scale adoption of domestic tech and fostering indigenous innovation.

Foreign Affairs | CSIS

AI, combined with advances in drones, sensors, and robotics, is lowering the barriers for terrorists and other non-state actors to conduct targeted attacks from a distance. Widely available tools, particularly open-source AI models that can run on inexpensive hardware, allow smaller groups with limited resources to deploy capabilities once largely reserved for state militaries. As a result, **AI is democratizing advanced violence** by expanding who can carry out technologically enabled attacks and how easily they can do so.

War on the Rocks

Foreign adversaries are increasingly using **AI-enabled cyberattacks against Western targets**. In 2025, Chinese operators reportedly used advanced AI models to conduct large-scale cyber operations with minimal human oversight. Iranian cyber groups have also intensified attacks using AI tools, especially after U.S. strikes began. The last example being a major cyberattack on the medical tech firm Stryker Corporation on March 11**.** These efforts target sensitive infrastructure such as **data centres, cloud systems, financial networks, and AI model repositories**.

Foreign Affairs | Wall Street Journal

Russia is restructuring its military C2 by shifting away from efforts to build a single, fully integrated digital command architecture and instead prioritising smaller, tactical software systems that directly improve battlefield performance. Wartime experience has accelerated this shift, particularly as unmanned systems now conduct a large share of fire missions, driving investment in software that links drone reconnaissance with artillery and other strike units to shorten the targeting cycle. AI is being applied mainly to tasks such as computer vision, sensor fusion, and target recognition, where it can analyse sensor data and support faster operational decisions. **Progress toward a fully integrated C2 system remains limited** by institutional barriers, fragmented data management, and the immature state of AI tools for decision support.

CSIS

Iran's retaliation during the first weeks of Operation Epic Fury demonstrates that **mass-produced drones have become central to modern air campaigns**, enabling sustained pressure at relatively low cost. During the first week of the conflict, drones accounted for roughly **71% of Iranian attacks**. The campaign relied on waves of low-cost **Shahed-series drones** to disrupt infrastructure and force defenders to expend expensive air-defence interceptors.

CSIS | Foreign Affairs

China has deployed converted Shenyang J-6 fighters as attack drones at air bases near the Taiwan Strait to support a potential first wave in a conflict. These drones, which are capable of supersonic speeds, are designed to be launched in large numbers to overwhelm air defences and force costly interceptions. They function more like expendable cruise missiles than traditional UAVs and form part of a broader, layered Chinese airpower strategy.

Reuters

Officials from U.S. Southern Command highlighted China's growing network of space-related facilities in South America, which could support satellite tracking, intelligence collection, and broader military operations under the guise of civilian use. At the same time, U.S. Northern Command warned that **China is deploying hypersonic glide vehicles and other advanced missile systems that can evade traditional defences, alongside space-linked capabilities such as orbital bombardment systems.** Together, these developments point to an increasingly integrated threat where space infrastructure and hypersonic weapons combine to enhance China's ability to detect, track, and strike U.S. targets with little warning.

Washington Times

China's upcoming 15th Five-Year Plan identifies **quantum technology as a major growth driver** alongside AI and biotechnology, with a shift from laboratory research to industrial deployment. This broader emphasis on frontier innovation also extends into security domains. Recent reporting indicates China is **exploring quantum sensing technologies**, such as advanced atomic magnetometers, to detect subtle underwater magnetic disturbances, potentially improving **submarine detection**, though these systems remain in the research and testing stage.

InfoseekChina | CGTN | 1945

China continues to lead as the **primary competitor in space** due to its scale, operating approximately **1,300 active spacecraft** as of late 2025, compared to Russia's 343. It appears to have developed a **near-continuous space-based surveillance capability over Japan**, with roughly 80 Yaogan satellites passing over key Japanese and U.S. bases about every 10 minutes, enabling **persistent monitoring of Allied deployments across strategic Indo-Pacific locations** such as Okinawa, Yokosuka, Sasebo, Taiwan, the South China Sea, and Guam. Recent developments

also include the **observation of a Chinese stealth satellite**, a capability typically associated with advanced military space operations. This expanding space capability is reinforced by **China's growing footprint in Africa**, where it is building ground stations, satellite partnerships, and broader space infrastructure that enhance global coverage and operational reach. By combining space diplomacy with control over critical mineral supply chains across the continent, China is strengthening both its space capabilities and its strategic leverage.

Space News | Yomiuri Shimbun | The Japan News | Atlantic Council

China is gaining advantage in AI-enabled biotechnology by systematically collecting and integrating large-scale biological datasets that feed AI development and industrial deployment. These coordinated biodata ecosystems allow faster progress in fields such as genomics, biomanufacturing, and medical research. **The convergence of AI and biotechnology has military value, enabling advances in biodefence, resilient bioindustrial supply chains, advanced biomaterials, and faster development of medical countermeasures.** The U.S, by contrast, lacks unified standards, secure compute-to-data systems, and coordinated national investment in high-quality, interoperable biodata, capabilities needed to build competitive AI-bio models.

War On the Rocks

Originator: HQSACT Innovation Branch, S&T Section

Version: March 2026

Contact: snt@act.nato.int | pietro.maccabelli@nato.int
