Panorama 2025 of Emerging Technologies for Defense

23/04/2025

Introduction

The digital revolution and the emergence of breakthrough technologies are profoundly reshaping the defense landscape. Anticipating developments over a 3 to 10-year horizon has become essential to maintaining strategic and operational superiority. This panorama of emerging technologies for defense responds to that need for foresight : it offers a structured analysis of weak signals and early trends that may shape tomorrow's defense capabilities. The methodology is grounded in internationally recognized foresight practices and has been adapted to the specific operational and industrial needs of defense stakeholders.

Founded in 2020, Mind2Shake is a catalyst for innovation serving both the defense sector and industry. We act as a bridge between innovators (startups, research labs...) and major institutional or industrial players. Our mission is to support innovation by grounding it in concrete use cases and keeping people at the center of transformation. This role as a catalyst is reflected in a pragmatic approach: breaking down organizational silos, fostering synergy, and accelerating the adoption of emerging technologies. In our strategic monitoring activities, we combine academic research methodologies with artificial intelligence to detect promising trends early and guide the decisions of our partners.

The structure of this document reflects that vision. The weak signals identified are grouped into key technological domains relevant to defense. For each domain, we highlight selected illustrative use cases to make the potential impact of these innovations tangible. These practical examples—without claiming to be exhaustive—shed light on the operational opportunities and challenges that lie ahead.

Credibility is central to our foresight approach: each weak signal presented is backed by reliable and diverse sources (scientific publications, official reports, technical analyses…). By consolidating high-quality references, we ensure that the trends highlighted in this panorama are grounded in verifiable facts, reinforcing the trust placed in our analysis.

Ultimately, our aim with this document is to provide decision-makers—whether from industry or the Ministry of the Armed Forces—with a decision-support tool that combines strategic vision with practical insight. This panorama offers a clear analytical framework for technological developments by 2030, helping guide today's investment and innovation decisions to ensure the technological superiority and sovereignty of tomorrow's defense sector.

Military Health

References :

- CRISPR Cas9 Gene Editing Market Size And Industry Report 2027
- (1) AMR Future Brief| The Pioneering Role of Biotechnology in Transforming Military Operations | LinkedIn
- NATO - Official text: Summary of NATO's Biotechnology and Human Enhancement Technologies Strategy, 12-Apr.-2024
- Super-soldiers: augmented humans in wartime - Polytechnique Insights
- Frontline Genomics: How Biotech is Becoming Integral to NatSec Strategy » Karve

Biotechnologies for Human Enhancement

Advances in genetics and biotechnology are paving the way for "augmented" soldiers. Techniques such as CRISPR and gene editing are being explored to enhance the physical and cognitive capabilities of warfighters, while epigenetic modulators could improve resistance to stress. In parallel, research on the microbiome (gut flora) and tailored probiotics aims to strengthen immune systems and psychological resilience in extreme environments. These approaches remain experimental and raise ethical considerations, but they could potentially revolutionize soldier preparation and conditioning.

Potential use cases: Pre-deployment administration of gene therapies to boost endurance or resistance to disease in soldiers, use of epigenetic supplements (molecules that regulate gene expression) to maintain composure and cognitive performance in high-stress combat scenarios, ingestion of custom-designed probiotics to enhance immunity and reduce stress during extended missions in harsh environments

Maturity level: Fundamental research and preclinical phase. Early animal studies and laboratory trials have shown promising effects, but the path to operational deployment remains long (≥ 5–10 year horizon). Armed forces and NATO are closely monitoring these developments while also assessing associated risks and legal implications.

In 2024, NATO emphasized that human enhancement technologies—such as exoskeletons and neuro-interfaces—offer clear opportunities, but also raise significant security and ethical challenges.

Médecine régénérative et bio-impression 3D

Medical biotechnologies are advancing toward emergency treatment solutions in the field that were once considered impossible. The 3D printing of biological tissues—bioprinting—is emerging as a way to produce skin, blood vessels, or even organs on-site to treat severe injuries without the need for immediate evacuation. For instance, military laboratories are experimenting with biologically active dressings embedded with a patient's own cells to accelerate the healing of burns. Likewise, stem cell therapies hold promise for regenerating damaged tissues (such as muscle or nerve cells), reducing long-term trauma in wounded soldiers.

Potential use cases : A deployable surgical module capable of 3D printing artificial skin or tissue fragments to treat gunshot wounds on-site, avoiding emergency evacuation, use of stem cells on the battlefield for accelerated bone or nerve reconstruction following trauma, reducing recovery time, local production of synthetic blood or bioprinted blood substitutes for transfusion in isolated zones (currently under research)

Maturity level: Prototype / laboratory demonstrator. Basic tissues and organoids have been successfully printed in laboratory settings, and some in vivo trials are currently underway. The U.S. military has funded pilot projects to develop deployable bioprinters. However, the full functional printing of complete organs remains a technical challenge for the next decade.

The literature indicates that bioprinting has "revolutionized field medicine by enabling on-site production of tissues and organs to treat severe injuries more effectively and reduce evacuations." Military medical research reports in 2024 confirm the rise of stem cell-based protocols to regenerate muscles and tissues in wounded personnel.

Wearable Biometric Sensors and AI-Enhanced Health

New wearable biosensors now enable continuous health monitoring for soldiers and provide early warnings in the event of injury or exposure to toxic agents. These devices—integrated into clothing, watches, or skin patches—track vital signs in real time (such as heart rate, stress levels, and blood glucose) and can detect anomalies like early-stage infections or the presence of chemical toxins. When coupled with artificial intelligence, they can process data from hundreds of soldiers simultaneously and predict emerging medical issues before they become critical. These AI-powered health systems also deliver personalized recommendations—hydration, rest, treatment—either directly to the soldier or to military medical staff.

Potential use cases : smart skin patch detecting exposure to a biological or chemical agent and instantly alerting the soldier and the command medic, uniform-integrated sensor monitoring fatigue and stress, providing unit commanders with a real-time exhaustion index to anticipate rotations, onboard AI diagnostic system in medical vehicles, analyzing data from connected helmets to prioritize evacuations through automated triage.

Maturity level : Field trials underway. Some armies are already testing connected watches and biometric belts on pilot units. Basic vital sign sensors (heart rate, sleep monitoring) are commercially available, but more advanced detectors (pathogens, toxins) remain at the lab prototype stage. The integration of AI for injury prediction is still in its early phase, with limited deployment expected within approximately 3 years.

Recent military programs highlight how sophisticated wearable biosensors are becoming—able to continuously monitor vital signs and even detect early signs of infection or intoxication. Moreover, AI is already being used to process these data and predict health problems before they escalate—such as anticipating heatstroke or musculoskeletal injuries by analyzing a soldier's biometric patterns.

Interfaces cerveau-machine et prothèses neuronales

In the fields of rehabilitation and human augmentation, neural interfaces connected directly to the brain are opening up new possibilities for treating injuries—and even for controlling systems. Implantable or external devices (such as advanced EEG headsets) allow severely injured soldiers to control robotic prosthetic limbs by thought, with enhanced precision and dexterity. These same interfaces could eventually be used to send mental commands to drones or ground robots—a concept currently being explored by DARPA. Meanwhile, advances in neural prosthetics are providing amputees with sensory feedback, allowing them to feel pressure or texture through artificial limbs connected to their nervous systems.

Potential use cases : enabling an amputee soldier to pilot a drone or ground vehicle using a neural interface, without using hands, to remain operational in a drone unit, equipping commandos with mind-controlled headsets to discreetly command swarms of micro-drones faster than by manual control (emerging technology), nerve-connected limb prosthetics that restore a sense of touch for wounded soldiers, significantly improving functional recovery

Maturity level : Experimental (TRL 4–5). Human trials have already demonstrated the feasibility of controlling an artificial arm by thought, or piloting a drone simulator via a brain-machine interface. However, these systems remain bulky and require a controlled environment. More portable and operational versions could emerge within 5 to 10 years for routine rehabilitation use. Their deployment in active operations—such as real-time system control—will depend on significant progress in reliability and cybersecurity (including protection against potential hacking of neural systems).

Reports from 2024 highlight rapid progress: "The development of neural interfaces that connect the brain directly to external devices is advancing quickly. These interfaces are already helping wounded soldiers regain lost functions and control advanced prosthetics with their minds." NATO has also emphasized the relevance of such technologies for rehabilitating military personnel and supporting their return to active duty following severe injury.

Logistics

References :

- Blockchain for military logistics | Article | The United States Army
- (2) The future of military logistics: how autonomous systems are shaping the battlefield of tomorrow | LinkedIn
- 524. Weapons on Demand: How 3D Printing Will Revolutionize Military Sustainment | Mad Scientist Laboratory
- Autonomous Vehicles: New Technology Revolutionizes Army's Principles of Sustainment | Article | The United States Army
- Ruggedized Bioprinter Successfully Prints Medical Products in Austere Environment - Geneva USA

Autonomous and Intelligent Logistics

Military logistics chains are becoming increasingly automated through the use of AI and robotics, ensuring the right supplies are delivered to the right place at the right time, without human intervention. Autonomous vehicles (driverless trucks) are currently being tested to form robotic convoys that deliver supplies along high-risk routes. Similarly, transport drones are being developed to carry medical equipment or ammunition over the last mile, bypassing obstacles on the ground. These systems reduce personnel exposure and increase responsiveness by minimizing human error. AI-powered logistics platforms also help optimize inventory and routing by predicting demand, managing smart warehouses, and coordinating resource allocation. In parallel, blockchain technologies are being explored to secure and trace logistics flows end-to-end, ensuring the integrity of critical supply chain data.

Potential use cases : convoys of autonomous trucks following a lead vehicle or fully AI-controlled, delivering fuel and rations to forward bases without the need for human escort, delivery drones airdropping medical supplies to isolated forward positions in hostile territory, avoiding exposure of helicopters and their crews, smart military warehouses where robots and AI systems autonomously manage inventory, packaging, and shipment of equipment to units, with blockchain ensuring end-to-end traceability and authenticity of parts

Maturity level : Advanced pilot programs. The US Army has already conducted several years of field testing for robotic truck convoys (Leader-Follower program). Demonstrator platforms for logistic drones also exist, and some have been deployed in real-world tests. Gradual adoption is expected within the next five years for non-critical support missions, as systems prove their reliability. AI-driven logistics planning is already embedded in some military information systems, but full autonomy—especially decision-making without human oversight—remains cautiously limited.

Military logistics experts describe "supply chain operations entirely managed by machines, from the warehouse to the front line. One can imagine bases nearly fully operated by AI systems capable of forecasting demand, allocating resources, and autonomously dispatching deliveries." The expected benefits include unprecedented levels of efficiency and reliability, by eliminating human error and delays.

Fabrication additive de pointe sur le terrain

3D printing (additive manufacturing) is emerging as a disruptive logistical solution, enabling the on-site production of spare parts and equipment on demand. Instead of waiting for long and risky supply chains, deployed forces will be able to locally manufacture weapon components, vehicle parts, or even entire drones. Rugged 3D printers—possibly containerized—can use secured digital files to produce anything from basic mechanical parts to more complex structures. This significantly shortens the supply chain and reduces dependence on rear bases. Meanwhile, advances in printable materials (advanced metals, composites, even printable explosives) are expanding the scope of applications. To ensure authenticity and quality, blockchain technologies can secure the "digital thread" of these parts, preventing design file tampering or unauthorized use.

Potential use cases : a frontline regiment prints a damaged tank part (gear, seal, etc.) in just a few hours from a 3D model sent from the rear, restoring vehicle availability without delay, on-site manufacturing of customized reconnaissance drones using raw materials and digital blueprints tailored to the local terrain, mobile 3D printing workshops embedded in containers and deployed near the front line to continuously produce specialty ammunition, critical spare parts, or emergency medical equipment (splints, prosthetics).

Maturity level : Rapid development. Both the US and French militaries have been experimenting with 3D printing in operational contexts for several years (e.g., printing helmets, vehicle components). As early as 2022–2023, makers were observed producing improvised weapons or drones using 3D printers in conflict zones. Today, the challenge lies in scaling these practices: deployable additive manufacturing units are in prototype stage, and the US Army is targeting generalized capacity by 2030. Ensuring machine reliability in field conditions and training personnel remain key challenges over the next 3–5 years.

A foresight report notes that "the 3D printing revolution is transforming logistics by enabling localized manufacturing and shortening the supply chain, thereby reducing vulnerability and delays." The US Army is considering a hybrid approach: storing only the most critical components while printing the rest on demand near the front line. Concrete examples from Ukraine and the Middle East already show combatants using 3D printers to produce weapons and drones in response to equipment shortages.

Advanced Sensors

References :

- DARPA eyeing new quantum sensing program | DefenseScoop
- (2) AMR Future Brief| The Pioneering Role of Biotechnology in Transforming Military Operations | LinkedIn
- 'Passive' Radar Can Give Soldiers Stealth in Urban Battlegrounds
- Armed with quantum sensors, France eyes leaps in electronic warfare
- NATO - News: Using quantum technologies to make communications secure, 27-Sep.-2022
- For Morphing Chem-Bio Threat, Best Defense Is More Defense
- Bringing New Technologies to Bear for Biosurveillance | RAND

Quantum Sensors for Navigation and Detection

Quantum sensors leverage the principles of quantum physics to achieve levels of sensitivity unattainable by traditional sensors. Within a 3–10 year timeframe, they could equip military platforms for two key applications: alternative PNT (Positioning, Navigation, and Timing) and stealth detection. For example, an ultra-precise quantum accelerometer or a quantum magnetic field sensor could allow a ship or aircraft to accurately determine its position by measuring anomalies in Earth's gravitational or magnetic fields—even in the event of GPS jamming. Similarly, next-generation quantum sensors may detect extremely subtle variations in electromagnetic or gravitational fields, revealing submarines, underground tunnels, or stealth aircraft previously undetectable. DARPA is investing in these capabilities through its RoQS (Robust Quantum Sensors) program, aimed at making such sensors resilient to field conditions such as vibration and interference.

Potential use cases: Quantum inertial navigation: a strategic submarine or missile equipped with a quantum navigation unit maintains precise heading with almost no drift, even without GPS, using ultra-stable gyroscopes and atomic clocks, Detection of underground structures: a surveillance aircraft equipped with a quantum gravimeter detects voids or bunkers below ground by measuring gravity anomalies, improving intelligence on hidden installations, Counter-stealth capability: a passive radar system paired with a quantum magnetic field sensor detects the presence of a stealth aircraft in flight by registering the minute disturbances it causes in Earth's magnetic field.

Maturity level: Laboratory prototype / early-stage industrialization. Quantum sensors (atomic clocks, gyroscopes) exist in laboratory settings with unmatched performance but are often bulky and sensitive to disruption. The current trend is toward miniaturization (e.g., portable cold-atom sensors). Demonstrations onboard military platforms are expected within 5 years, with isolated operational deployments—particularly for submarine navigation—likely within the 10-year horizon.

The Pentagon already considers quantum sensors to offer promising capabilities for alternative navigation and ISR (intelligence, surveillance, reconnaissance). A 2024 article highlights that while these sensors have proven their accuracy in the lab (measuring magnetic, rotational, or gravitational fields), they must now be adapted for deployment on real-world platforms—precisely the objective of DARPA's RoQS program. The goal is to preserve quantum performance even in dynamic, rugged environments and deliver a significant technological edge to the Department of Defense.

Biosensors and Next-Generation Chemical Detectors

The CBRN threat (chemical, biological, radiological, nuclear) demands increasingly responsive and sensitive detection systems. One emerging trend is the use of bio-inspired or living systems for detection. Researchers are developing synthetic microorganisms programmed to react to the presence of toxins or pathogens by emitting a measurable signal. These biosensors could be deployed in the field (as sensor strips, dispersible powders, etc.) to provide early warning of chemical or biological attacks. In parallel, electronic sensors are advancing: new hyperspectral and infrared detectors—enhanced by materials such as graphene or metamaterials—may identify chemical signatures at a distance or through barriers. Passive systems are also on the rise, such as passive radar or acoustic sensors that rely on ambient radio waves or sound to detect threats without emitting any signal. This is especially valuable in urban settings or for special forces seeking stealth.

Potential use cases: Deployable biosensor networks: small field-deployable sensors embedded with modified bacteria that glow or change color upon detecting a nerve agent, providing near-instant chemical mapping for troops, Multispectral portable detector: a soldier uses a handheld graphene-based sensor to scan a building and detect explosives or chemical residues through walls, Pocket-sized passive radar: a lightweight device captures ambient FM or TV radio waves to track the movement of enemy drones in urban terrain without emitting any signal, ensuring stealth

Maturity level : Varies depending on technology. Traditional electronic chemical detectors are already in use, but next-generation variants based on nanomaterials like graphene are in advanced prototype stages. Biosensors remain in applied research: some have shown successful detection in controlled environments, but operational deployment faces hurdles such as microbial longevity and false positives. First hybrid systems (biological elements + electronics) could be tested in field conditions within 5 years. Passive radar is already proven in the civilian sector, and militarized versions for urban drone detection are likely to be adopted soon.

Publications emphasize that wearable biosensors and biological detection systems are redefining CBRN defense: "Portable biosensors capable of continuously detecting toxins or early signs of infection… environmental detectors identifying chemical, biological, or radiological agents in the field for early warning." The rise of passive sensors is also noted: one defense outlet describes a passive radar system leveraging civilian radio waves to provide the same targeting data as conventional radar (range, velocity) without emitting a signal—ideal for stealth detection of drones and aircraft in contested environments.

Advanced Materials

References :

- Advancing Stealth: Chinese Scientists Develop Meta-Materials-Based Radar Cloaks – International Defense Security & Technology
- Army Researchers Dream New Self-Healing Material Will Lead to 'Terminator' Technology | Military.com
- (3) AMR Future Brief| The Pioneering Role of Biotechnology in Transforming Military Operations | LinkedIn
- https://www.defenseone.com/technology/2015/10/military-wants-vampire-drones-die-sun/122722/

Stealth and Multifunctional Metamaterials

Metamaterials are engineered materials designed to manipulate waves—electromagnetic, acoustic, or otherwise—in ways not achievable with conventional materials. In defense applications, they pave the way for a new generation of stealth coatings and compact antennas. Metamaterials based on printed resonant structures could render an object nearly invisible across wide radar frequency bands by bending electromagnetic waves around it—the once-fictional "invisibility cloak" is now credible for certain use cases. Unlike traditional stealth coatings limited to narrow bands, these ultra-thin absorbers can function effectively across radar L to X bands without compromising aerodynamics. Metamaterials are also being used to create ultrathin, high-gain antennas for communications and electronic warfare, and even thermal shielding systems for infrared camouflage. China, in particular, claims major advances by integrating metamaterials into its aircraft, reducing radar signatures by 10 to 30 dB across broad frequency ranges. These materials can also increase strength and reduce weight through structures like honeycomb lattices.

Potential use cases : Adaptive stealth coatings: applying metamaterial-based films to drones to absorb or deflect radar signals across all major military radar bands, making them virtually undetectable while keeping the airframe lightweight, Integrated metamaterial antennas: embedding flat, high-gain antennas into the fuselage of aircraft to enable long-range communications or directional jamming without protruding hardware, Thermal camouflage for vehicles: coating armored vehicles with optical metamaterials that dynamically adjust their visual and infrared signatures (e.g., mimicking ambient temperature) to blend into surroundings and avoid thermal imaging detection

Maturity level: Transitioning from lab to field. Since initial proof-of-concept demonstrations in the early 2000s, researchers have developed 2D radar cloaks and small-scale functional antennas. Some fifth-generation fighter jets may already use metamaterial elements in classified subsystems. Intense R&D is underway. Within 3–5 years, we can expect modular metamaterial kits to be tested on existing platforms to assess stealth gains. Broad operational use will follow once costs decrease and durability under combat conditions is proven.

Metamaterials are now seen as transformational stealth technologies, offering unprecedented control over wave propagation. Analysts suggest that "ultra-thin, broadband absorbers and even optical cloaking devices are now within reach." Chinese sources report breakthroughs in tunable metamaterial surfaces, enabling aircraft to become lighter, stealthier, and more affordable. Additionally, incorporating metamaterials into communication systems enhances range and precision for jamming while simultaneously reducing infrared signatures—confirming their status as dual-function enablers.

Self-Healing and Adaptive Materials

Inspired by nature (like skin or bone), researchers are developing materials capable of repairing themselves after being damaged. For example, the U.S. Army has created a new 3D-printable epoxy polymer that can reconfigure and regenerate automatically when cracked or punctured. In the future, such materials could provide drones and robots with a form of "Terminator-like" resilience: if a drone wing fractures mid-flight, the material re-bonds itself; if a robot takes an impact, its polymer shell absorbs the shock and then heals. Some of these materials also have shape memory—meaning they respond to stimuli (heat, magnetic field) by changing shape and then reverting to their original form. When combined with embedded sensors, these are called “smart materials,” capable of adapting to their environment without human input. For instance, armor plating could harden or soften in anticipation of an impact. These innovations are designed to increase equipment longevity and reduce the need for maintenance in the field.

Potential use cases: Self-healing reconnaissance drone: a drone with flexible wings made from self-repairing materials that automatically mend minor tears caused by obstacles, allowing it to resume its mission within minutes, Autonomous ground vehicle armor: a vehicle shell made from special polymers that seal bullet holes or shrapnel damage, maintaining internal system protection in combat, Additively manufactured firearm components: parts printed using self-healing composites that extend the weapon's service life by resisting wear and regenerating after thermal stress (e.g., suppressors)

Maturity level : Applied research / early prototyping. Initial self-healing materials exist—such as polymer coatings that close up when exposed to heat or moisture. In the civilian sector, self-healing concrete and automotive paints are already being tested. In defense, the U.S. Army Research Lab (ARL) presented a 3D-printable, shape-shifting polymer in 2020. Current demonstrations focus on small parts that re-seal or reconfigure. Full integration into complex systems like drones or robots could be feasible within 5 years for basic features. The long-term vision—quasi-organic platforms able to autonomously reshape and repair like the T-1000 in Terminator 2—is likely 10+ years away and dependent on further breakthroughs in material chemistry and embedded energy systems.

A Military.com article highlighted that ARL and Texas A&M are developing “a 3D-printable polymer that can change shape and heal itself,” envisioned for future aerial and robotic platforms. The lead researcher likened this material to the T-1000’s reconfigurable body in Terminator 2, illustrating the ambition: a structural material that simultaneously supports, senses, and adapts—responding autonomously to damage without external control.

Bio-Based and Transient (Ephemeral) Materials

Two complementary trends are emerging: the use of bio-based materials for military equipment, and the development of transient materials that intentionally disappear after use. On one hand, biosynthetic processes allow the production of high-performance materials—for example, body armor made from spider silk-inspired biopolymers offers high protection while being lighter and more flexible than traditional Kevlar. Equipment or protective gear could be "grown" by microorganisms, lowering costs and reducing dependence on critical raw materials. On the other hand, the operational need to leave no trace on the battlefield has led DARPA to launch programs such as VAPR and ICARUS, aimed at creating self-destructing drones and sensors. These systems are designed using materials (particularly polymers) that degrade within hours—either on command or after a set period—leaving behind little to no detectable residue. One example is a mini delivery drone whose special polymer frame sublimates into gas at sunrise, preventing it from falling into enemy hands. These ephemeral materials help ensure logistical stealth and protect sensitive technologies from recovery or exploitation.

Potential use cases : Bio-based ballistic vest: a bulletproof vest woven from synthetic spider silk that offers lightweight, high-performance protection; after use, it can be composted or thermally dissolved to reduce logistical footprint, Single-use delivery drone: dropped at night with critical supplies (e.g., blood packs), it self-destructs at sunrise—its structure vaporizing silently within ~30 minutes to avoid detection or capture, Disposable surveillance sensors: small audio/video sensors deployed in enemy territory, fabricated from transient electronics on silk or dissolvable glass substrates; they collect intel for 24 hours then dissolve with moisture, leaving no trace

Maturity level : Notable recent progress. Bio-based materials are already in use for some applications (e.g., flax fiber in composites). High-strength biopolymers like synthetic spider silk remain costly but are seeing improving fabrication techniques (with potential applications in high-performance military textiles within 3–5 years). Transient materials have seen real-world demonstrations: DARPA announced as early as 2015 that it had succeeded in making small polymer structures and fragile electronics disappear. In 2020, a prototype drone demonstrated partial self-disintegration. We can expect deployable ephemeral sensors for special forces within 2–3 years. Fully vanishing drones capable of flight and self-erasure remain more complex, but a prototype could realistically emerge by ~2030.

An Allied Market Research report notes "the development of biosynthetic materials, such as armor and garments made from biopolymers, offering enhanced protection and durability on the battlefield." Regarding transient materials, DARPA's ICARUS program received wide coverage: "designing delivery aircraft that disappear within four hours of completing their mission... relying on advancements in sublimating polymers (solid-to-gas)." Defense One described these as "vampire drones that die at sunrise," capturing the core principle of temporary, untraceable assets.

Cybersecurity

References :

- https://defensescoop.com/2024/10/24/dod-cryptographic-modernization-effort-challenges/
- Pentagon Warns AI Warfare Risks Unknown, Launches SABER Program to 'Red Team' AI Battlefield Systems - The Debrief
- DARPA Selects Researchers to Accelerate Use of Fully Homomorphic Encryption
- Silent Swarm Exercise Accelerates Navy's Path To Distributed Electronic Warfare Future
- AI in Defense: Navigating Concerns, Seizing Opportunities

Post-Quantum Cryptography and Secure Communications

The rise of quantum computing presents a medium-term threat to current encryption standards. An adversary with quantum capabilities could break communications previously considered secure within hours. In response, a major cryptographic migration effort is underway: newly standardized post-quantum cryptographic (PQC) algorithms are being developed and must be deployed before this threat becomes reality. These algorithms (e.g., CRYSTALS-Kyber, Dilithium) are designed to resist known quantum attacks and will replace RSA, Diffie-Hellman, and similar methods across military systems. The challenge is vast—requiring updates to millions of devices and networks, from strategic infrastructure to tactical radios. At the same time, quantum communication technologies (like Quantum Key Distribution, QKD) are being explored for ultra-sensitive links, providing provable security (any interception disrupts the message). Additional techniques—such as dual encryption (double-wrap) and running multiple cryptographic schemes in parallel—are also being considered to build transitional resilience. The overarching objective is to stay ahead of adversarial computational capabilities.

Potential use cases : Upgrading military communications networks (e.g., satellites, radios) to use post-quantum cryptographic suites: a tactical radio in the field exchanges keys via Kyber instead of traditional Diffie-Hellman, Secured strategic communications over quantum links: a fiber-optic cable between two command centers uses Quantum Key Distribution (QKD) to securely transmit keys, ensuring the confidentiality of launch orders or mission-critical data, Homomorphic encryption in intelligence workflows: classified data remains encrypted even during processing on shared or cloud platforms, as fully homomorphic algorithms enable computation without decryption—critical for safeguarding sensitive operations.

Maturity level : Standardization ongoing, initial deployments underway. In 2024, NIST finalized its first set of post-quantum cryptographic algorithms. The U.S. Department of Defense is planning to migrate its critical systems to these standards by 2035—a tight schedule given the scale of the update. Some newer systems already include PQC-based prototypes. Quantum communication (e.g., QKD) remains limited to demonstrations over short fiber distances or via experimental satellites. Broader adoption on fixed government links may occur within 5–10 years. Fully homomorphic encryption (FHE) is less mature: DARPA's DPRIVE program is currently working to reduce the computational cost through hardware acceleration, with early hardware prototypes under evaluation.

According to DefenseScoop, the Pentagon's Deputy CIO emphasized that "cryptographic modernization is now a top priority," citing the urgent need to "develop quantum-resistant algorithms before our adversaries can exploit the gap." In August 2024, NIST finalized three post-quantum algorithms, targeting migration of critical systems by 2035. DARPA has also highlighted the strategic value of homomorphic encryption, enabling data to remain protected "at rest, in transit, and in use," although adoption will depend on breakthroughs in performance and hardware acceleration.

IA offensive, attaques adversariales et cyberdéfense de l'IA

Artificial intelligence is not only beneficial—it is increasingly becoming a double-edged sword in cyberspace. New threats are emerging, such as adversarial attacks targeting AI systems: an enemy can exploit the weaknesses of vision or decision-making algorithms (e.g., by manipulating input data) to deceive or disable them. This could cause a system to misidentify a target or neutralize an autonomous vehicle. In response, DARPA launched the SABER program to assemble a specialized AI red teaming unit tasked with attacking our own AI systems to uncover vulnerabilities before adversaries do. At the same time, malicious actors are leveraging AI themselves—generating increasingly realistic deepfakes for influence campaigns or identity theft, crafting adaptive AI-driven malware, or automating the discovery of zero-day exploits using intelligent search algorithms. In turn, cyberdefense strategies are evolving by integrating AI into detection mechanisms (anomaly detection via machine learning, automated behavioral analysis) and by developing countermeasures against adversarial AI attacks (robust AI models, adversarial filters). There is also growing emphasis on extending Zero Trust principles to AI itself—ensuring the integrity and authenticity of deployed models (e.g., verifying no adversarial backdoors exist).

Potential use cases : State-sponsored hackers use malicious LLMs to generate highly personalized and virtually undetectable phishing emails targeting military personnel—forcing cybersecurity teams to enhance filters and phishing awareness training with AI-based defenses, Adversarial input attacks in combat zones: an adversary broadcasts deceptive signals or imagery specifically crafted to fool autonomous targeting systems, causing them to misclassify friendlies or fail to detect camouflaged enemies, AI red teaming units embedded in defense R&D organizations conduct simulated attacks on new robotic or autonomous systems to identify and patch AI vulnerabilities before deployment.

Maturity level : Emerging threat, increasing awareness. Successful adversarial attacks have been demonstrated in lab environments, including against autonomous vehicles and computer vision systems. Although no confirmed large-scale adversarial AI use in combat has been reported, the U.S. Department of Defense considers it an imminent risk. Since 2023–2024, directives from the DoD and DHS have emphasized the need to harden AI models and monitor malicious use of generative AI. Real-world incidents involving deepfakes or AI deception are expected within 1–3 years—if they haven't already occurred covertly. The race between offensive and defensive AI is fully underway.

In 2024, DARPA noted: "Adversarial AI attacks, once considered theoretical, have yet to be seen in combat operations, so risks remain poorly understood. That's why we launched SABER—to proactively test and secure battlefield AI systems." The SABER program will bring together experts to conduct adversarial red teaming of autonomous defense platforms. Meanwhile, the U.S. Department of Homeland Security warned that adversaries will "leverage AI to create more credible disinformation and sophisticated cyberattacks"—prompting urgent investment in AI-based countermeasures.

Energy

References :

- Department of Defense Breaks Ground on Project Pele Microreactor | Department of Energy
- U.S. Army Seeks Microreactor Nuclear Power Plant Solutions for Military Bases | Microgrid Knowledge
- Raytheon to Build Power Beaming Solutions for US Army
- POWER Program Selects Teams to Design Power Beaming Relays
- Batteries as a Military Enabler - War on the Rocks
- Rechargeable Lithium Metal Battery Technology Revolutionizes Drone Capabilities for Defense Applications | AUVSI
- Israeli Firm Unveils 'Groundbreaking' Military Battery System

Portable Nuclear Micro-Reactors

To ensure a reliable and continuous energy source in remote operational theaters, armed forces are turning to portable nuclear micro-reactors. These compact reactors—generating a few megawatts—are designed to fit within standard shipping containers and provide electricity to forward bases for several years without requiring fuel resupply. U.S.-led projects like Project Pele are developing high-flux, gas-cooled micro-reactors that can be transported by road or aircraft. The goal is to power high-demand military systems (radars, lasers), critical communications, and life support while drastically reducing fuel convoys—one of the most vulnerable elements in logistics. These reactors incorporate advanced passive safety features to prevent accidents (e.g., automatic shutdown in case of malfunction) and shielding to protect against attack. Prototype deployment is expected by 2030 at selected test sites. If these miniature reactors live up to expectations, they could revolutionize military energy logistics by providing abundant, on-site power without dependency on external fuel sources.

Potential use cases : Remote base energy autonomy: a 5 MW micro-reactor deployed at an isolated operational base (e.g., in Arctic or desert conditions) powers anti-aircraft systems, water desalination, drone charging stations, and command infrastructure without a single liter of fuel being convoyed, Disaster response support: in the aftermath of a natural disaster, a military-deployed micro-reactor restores power to critical infrastructure such as an airport or field hospital, ensuring continuity of humanitarian or stabilization missions, Naval or autonomous surface vessels: smaller vessels equipped with micro-reactors instead of traditional engines gain long-duration, fuel-independent operational capabilities—ideal for drone carriers or persistent ISR platforms.

Maturity level : Near-prototype stage. The U.S. Department of Defense has launched formal calls for proposals and expects to deploy a prototype micro-reactor at a domestic military base by 2030. Project Pele completed detailed design phases by 2022, with construction beginning in 2023. Russia and China are also developing mobile reactor systems, particularly for Arctic or expeditionary use. Real-world implementation still depends on demonstrating operational safety, transportability, and end-of-life handling. A first wave of experimental deployment at forward sites is expected before large-scale adoption.

According to Microgrid Knowledge, "the military plans to deploy a micro-reactor prototype at a U.S. facility by 2030. If successful, the technology could be used on bases worldwide." The Department of Defense sees this as a critical step to strengthen energy resilience at installations vulnerable to disruption. The U.S. Congress has also emphasized the strategic importance of securing uninterrupted power supply for austere environments via such mobile, carbon-free reactors.

cdr@mind2shake.com
Agitateur & Innovations
71/73 rue Desnouettes 75015 Paris
SIRET | 888 850 815 00026

Wireless Energy Transmission

Directed energy isn't just for weapons—it's also a promising way to transmit power. The concept involves delivering electricity to a distant system via a laser or microwave beam, eliminating the need for cables or bulky batteries. In 2024, the U.S. Army awarded a contract for the development of power-beaming systems capable of transmitting kilowatts over several kilometers. In practice, a transmitting station converts electricity into a tightly focused laser beam (infrared or microwave) and directs it at a receiving device—typically a specialized photovoltaic panel or antenna—that reconverts the beam into usable electric power. This technology could enable mid-air refueling of electric drones, permanent power supply to elevated sensors, or energy delivery from an aircraft or satellite to a forward unit on the ground. The strategic advantages are significant: less fuel and fewer batteries to transport, energy supply from the rear without exposing assets, and greater operational autonomy in austere environments. Current efforts focus on improving conversion efficiency and ensuring safety—particularly avoiding harm to personnel or equipment that might intersect the beam.

Potential use cases : Drone swarms recharged in flight: a high-altitude aircraft acts as an energy relay, sweeping the sky with a power-beaming laser that extends the mission endurance of electric surveillance drones indefinitely, Forward base supply from rear HQ: a ground relay system transmits 10 kW of energy via laser across 50 km, through a network of optical mirrors, from a protected rear generator to a front-line command post without logistics convoys, Battery-free field sensors: sensors deployed in enemy territory operate autonomously, receiving periodic energy bursts from passing drones or satellites via microwave beams, thus eliminating the need for battery swaps.

Maturity level : Initial demonstration stage. DARPA launched the POWER program in 2022 to develop airborne optical relays capable of transmitting around 10 kW over extended distances. In 2023, tests successfully delivered a few kilowatts via laser over a 1 km span to power a hovering drone. In late 2024, Raytheon was awarded a contract to scale and ruggedize these systems for U.S. Army deployment. Limited field use cases—such as charging small drones from a ground station—may emerge within 3–5 years. Delivering higher power levels over longer distances with precision and safety remains a challenge, especially under adverse weather or in contested environments. Nevertheless, point-to-point energy delivery for niche missions is plausible by the end of the decade.

A November 2024 briefing confirmed that "the DoD has tasked Raytheon with developing wireless power transmission systems for the U.S. Army." The aim is to create transmitters and receivers capable of reliable long-distance tests, supporting both manned and unmanned systems. Raytheon stated that this capability "will reduce the need for fuel and battery logistics, optimize mission duration, and lower dependence on vulnerable supply chains." These developments align with the Pentagon's broader energy strategy, including DARPA's POWER program for airborne energy relays initiated in 2022.

Next-Generation Energy Storage (Advanced Batteries)

Batteries have become critical for powering drones, electric vehicles, soldier-borne equipment, and directed energy weapons. Next-generation batteries aim to deliver much greater energy and power density at the same or lower weight—while also improving safety. Emerging technologies include solid-state batteries, which promise energy densities 50% higher than current lithium-ion systems and reduced fire risk. Other chemistries such as lithium-sulfur and lithium-air are being studied for energy densities two to five times greater, enabling, for example, drones to fly 70% longer or radios to operate for several days without recharging. In parallel, advances in battery architecture—such as electrode nanostructuring and bipolar designs—are increasing discharge power, which is essential for high-energy applications like mobile lasers and radar systems. Supply chain security is also a priority: reducing reliance on critical materials like cobalt or nickel, and diversifying sources, is becoming strategic. Finally, defense agencies are investing in diagnostics and thermal resilience to extend battery life in extreme conditions—from polar cold to desert heat.

Potential use cases: Electric combat drone with enhanced endurance: powered by solid-state batteries offering 50% more energy than lithium-ion equivalents, enabling 12-hour flights instead of 8, Mobile directed energy weapons: mounted on tactical vehicles, powered by high-discharge-rate batteries capable of firing multiple laser pulses without external generators, Soldier equipment modernization: thanks to lithium-sulfur batteries, each soldier carries a power pack half the weight of current versions, supporting radios, sensors, and night vision gear for extended missions without resupply.

Maturity level : Actively under development. Solid-state batteries are in advanced prototyping for automotive use, with commercial deployment targeted for 2025–2026. Militarized versions may follow shortly (2025–2027 testing expected). Lithium-sulfur chemistry

cdr@mind2shake.com
Agitateur & Innovations
71/73 rue Desnouettes 75015 Paris
SIRET | 888 850 815 00026

has already been tested on experimental drones. The UK and others have launched qualification programs for aerospace and military environments over the next 5 years. Incremental innovations are ongoing: in 2024, an Israeli company unveiled a military-grade 6T battery delivering six times the energy of a standard lead-acid version, and 50% more than competing lithium-ion models. The U.S. Defense Innovation Unit (DIU) also launched initiatives in 2024 to fast-track adoption of high-performance, ruggedized commercial batteries suitable for harsh operational environments. Expect fielded gains within 3 years, and more disruptive breakthroughs (solid-state, lithium-air) by the end of the decade.

A strategic analysis highlights that "the free world must scale up battery capacity and pursue breakthroughs like solid-state batteries, which could be game-changers both commercially and militarily." In 2024, an Israeli firm presented a standardized 6T vehicle battery delivering 4,400 Wh—six times that of lead-acid equivalents and significantly outperforming other lithium-based competitors. The DIU's energy director stated: "We've never been great at batteries—we used to build expensive custom systems. Now, we're switching to best-in-class commercial tech adapted to military use," underscoring the urgent need to counterbalance Chinese dominance in the global battery market.

Autonomous Systems

Sources :

- Drone Wars: Developments in Drone Swarm Technology - Defense Security Monitor
- USAF 'Loyal Wingmen' Receive Fighter Drone Designations for First Time
- From drone swarms to exoskeletons, Army charts path for robotic future
- Thales Unveils Next-Generation Autonomous Drone Swarms Powered by AI

Drone Swarms and Collaborative Combat

We are witnessing the rise of drone swarms capable of operating collectively and autonomously—ushering in a new form of digital superiority on the battlefield. A swarm typically consists of dozens or even hundreds of drones (aerial, ground, or maritime) coordinated by swarm intelligence algorithms inspired by bee colonies or ant networks. Rather than being piloted individually, these drones communicate among themselves to distribute tasks (reconnaissance, saturation strikes, jamming, logistics), adapt to losses and obstacles, and operate with minimal human supervision. Recent conflicts have demonstrated the decisive impact of integrated drone deployments, prompting armed forces to invest in unified control systems. For example, Sweden is testing an interface that allows a single soldier to control up to 100 drones simultaneously using grouped commands. In the United States, the Replicator program aims to deploy thousands of inexpensive, autonomous drones by 2025 to overwhelm adversary defenses through volume. When paired with manned platforms (as in the "loyal wingman" concept, where a drone flies alongside a piloted fighter), collaborative swarms promise to redefine military doctrine—enabling high-impact, multi-domain operations at a fraction of traditional cost.

Potential use cases :Swarming loitering munitions: an aerial swarm of 200 small, low-cost kamikaze drones is launched against a formation of armored vehicles. While many are intercepted, the swarm's collective intelligence identifies gaps in defense, allowing a sufficient number to strike effectively at a cost far below that of traditional munitions, Distributed reconnaissance: dozens of aerial and ground drones collaborate autonomously to map and monitor an urban area, sharing scanned sectors and detected targets without centralized control—ensuring full coverage while reducing latency, Loyal wingmen for manned fighters: an F-35 flies with two autonomous combat drones. The drones execute pilot-designated tasks such as electronic warfare or target engagement and can sacrifice themselves to protect the human pilot if needed.

Maturity level : Currently in field demonstration phase. Core swarm algorithms have existed for several years (e.g., the 2016 Perdix swarm dropped by F-18s). Since then, swarm capacity has scaled up significantly—China has demonstrated 40-drone formations; Sweden is testing control of 100 drones by a single operator. The U.S. Replicator initiative is accelerating toward near-term deployment (starting in 2025). Operational use of autonomous swarms in combat—particularly for kamikaze or ISR purposes—is likely within 1–3 years. The main challenges are no longer technological but operational: securing communications, ensuring system resilience under electronic warfare, and framing autonomous rules of engagement. As for loyal wingmen, two U.S. prototypes have already flown and received official designations (YFQ-42 and YFQ-44), with initial deployment targeted around 2028. Australia and several European countries are also pursuing demonstrators.

According to the U.S. GAO, a drone swarm is defined as "at least three drones operating with minimal human input, executing a shared mission using coordination algorithms." Forecast International reported in early 2025 that Sweden unveiled a program allowing one soldier to control 100 drones, with full-scale urban trials planned. Strategically, swarms promise to shift military balance by enabling low-cost saturation tactics that can defeat far more expensive defenses. The U.S. Air Force, having designated its first loyal wingman drones, described this as "symbolic of a new era in air combat—one that combines human decision-making with autonomous capability."

Autonomous Ground Vehicles and Robotic Systems

On the ground, autonomy is also advancing—from transport robots to unmanned combat vehicles. Armed forces are increasingly integrating robotic platforms to relieve soldiers from burdensome or high-risk tasks. For instance, the SMET/DUST program includes small autonomous vehicles that follow infantry units while carrying supplies (ammunition, water, batteries), or evacuate wounded personnel. Automated supply convoys are also under testing: a lead truck driven by a human is followed by 3–4 autonomous "follower" trucks, reducing troop exposure along logistics routes. In combat roles, we are seeing the emergence of armed UGVs (Unmanned Ground Vehicles), ranging from small tracked anti-tank robots to buggy-sized vehicles fitted with remote-controlled weapon stations. In the future, these robots could lead assaults as forward scouts or fire support, controlled from behind by human units. Interoperability is a key focus: the U.S. Army is developing a common architecture (CMOSS) to enable seamless sensor and control integration between aerial drones, ground robots, and connected soldiers. Finally, exoskeletons—though worn by humans—are part of this robotic family: motorized frames that lighten infantry loads or enhance strength are under evaluation to improve endurance and reduce injuries.

Potential use cases : Robotic logistics convoys: a column of supply trucks crosses an IED-threatened zone with only the lead vehicle manned. The rest of the convoy—autonomous followers—operates on preloaded routes or remote command, minimizing risk to personnel, Infantry robotic mule: a wheeled robot follows an infantry section, carrying up to 200 kg of gear. It tracks the squad leader via signal or GPS and can return autonomously to resupply or recharge, Armed ground drones for urban combat: lightweight tracked UGVs equipped with machine guns lead the way through narrow alleys, engaging ambushers while soldiers follow at a safer distance. Their onboard AI assists with obstacle avoidance and target recognition.

Maturity level: Continuous progress, initial field adoption. The French Army deployed robotic mules (e.g., Nexter's Optio) in Mali for evaluation. The U.S. Army has already reached short-term objectives with logistics and EOD (Explosive Ordnance Disposal) robots since 2017. Automated convoys have accumulated thousands of kilometers in testing, and limited real-world use is expected within 2–3 years, particularly for logistics. Armed UGVs remain in prototype phase: Russia fielded the Uran-9 in Syria with mixed results, but development continues. Within 5 years, combat-capable robots could be integrated into support roles in forward units. Exoskeletons showed mixed results in early trials due to bulk and complexity, but newer lightweight models are in testing in Canada, France, and beyond. Widespread adoption (e.g., for logistics or medical recovery) remains a 10-year horizon.

As reported by DefenseNews, "from drone swarms to exoskeletons, the Army is mapping out a robotic future." The 2017 U.S. RAS strategy already achieved several goals such as reducing soldier burden and automating partial logistics. In 2024, Army robotics lead Stuart Hatfield outlined active programs including tethered drones, autonomous aerial resupply systems, medium-lift transport robots, DUST robotic mules, first-person-view reconnaissance drones, and exoskeleton trials. This illustrates the growing diversity of ground robotics initiatives—many of which are nearing tactical integration. The emerging trend is clear: increasing the number of robots per unit and improving man-machine teaming will be decisive for tactical superiority.

Mind2Shake
cdr@mind2shake.com
Agitateur & Innovations
71/73 rue Desnouettes 75015 Paris
SIRET | 888 850 815 00026