



2027 Challenge: **Scalable and** **Adaptable** **Countermeasures** **for Air Defence**



Scalable and Adaptable Countermeasures for Air Defence

1. Challenge Summary: Current countermeasures to aerial threats face increasing limitations when confronted with massed combinations of low-cost unmanned systems, missiles and loitering munitions, as well as the saturation of sensor and command-and-control (C2) networks. A further challenge is the rise of deep, stand-off precision-strike threats, including cruise missiles and coordinated long-range strikes, supported by electronic warfare operations such as jamming and spoofing.


The Alliance is seeking modular, scalable, adaptable and data-integrated countermeasure solutions to protect manoeuvre forces, command posts, logistics hubs and key infrastructure against aerial threats. Solutions must perform in hostile electromagnetic environments characterised by electronic warfare and cyber-attacks, and be resistant to non-conventional effects such as laser weapons. Solutions should prioritise multi-sensor detection and data fusion into a shared air picture. Resilient C2 systems, interoperable architectures for coalition operations, and space-based early detection and warning systems are also required as key enablers of the Integrated Air and Missile Defence process.

2. Illustrative Scenario: During rapid reinforcement, a manoeuvre brigade establishes a forward command post near critical infrastructure. An adversary conducts a coordinated campaign designed to overwhelm local defences. Large numbers of low-cost unmanned systems are employed to saturate sensors, C2 systems, and deplete interceptor capacity. This is followed by coordinated long-range strikes, including cruise missiles and long-range fires, against C2 and air defence nodes, bridges, and fuel sites. Simultaneously, the adversary degrades the defenders' electromagnetic environment, launches cyber-attacks on C2 networks, and deploys high-power electromagnetic weapons to saturate sensors and disable sensor networks.

A shared air picture, enabled by the fusion of diverse sensor feeds and supported by space-based detection and warning systems, is used to coordinate a layered and scalable countermeasure response. This consists of kinetic and non-kinetic kill options that are deployed to neutralise the threats, despite the heavy electromagnetic spectrum contestation. The brigade protects its personnel whilst maintaining interceptor capacity, enabling effective defence for critical assets.

3. Exemplar Enabling Technologies: The following list provides illustrative examples of technologies that may contribute to this challenge. The list is not exhaustive, and NATO DIANA encourages integrated and novel approaches that extend beyond it:

Sensing, Detection and Early Warning

- 
- Low-cost active and passive sensing technologies (e.g. electro-optical, infrared, acoustic, radio-frequency) that enable the persistent detection, tracking and classification of small unmanned aerial systems and other low-signature threats in cluttered operating environments.
 - Multi-sensor fusion and methods to determine when different observations relate to the same threat, enabling a shared, resilient, and high-confidence air picture from heterogeneous coalition sensors, including under saturation.
 - Space-enabled sensing, early warning and space situational awareness services that provide cueing, detection, and attribution of precision-strike threats in support of integrated air and missile defence decision-making.

Scalable Countermeasures and System Resilience

- Scalable non-kinetic countermeasure solutions that disrupt or deny access to the electromagnetic spectrum or satellite navigation systems, including protocol-aware intervention and spoofing detection and mitigation to counter massed, low-cost UAS without reliance on limited interceptor stocks.
- Scalable hard defeat mechanisms, including low-cost interceptors and alternative effectors that enable a layered defensive approach when responding to high-volume and saturation attacks.
- Solutions for system hardening and graceful degradation, such as electromagnetic shielding and cyber-resilient components, that enable sensors and C2 nodes to remain effective under high-power electromagnetic and directed-energy effects.

Modular and Scalable Architectures

- Rapidly deployable and reconfigurable countermeasure modules that allow air-defence units to adapt combinations of sensors and effectors to local threat conditions and available resources.
- Modular open architectures and common interfaces enabling the rapid integration, interchange and reconfiguration of sensors, effectors and software across different vendors and nations.

Command, Control and Decision-Making

- Resilient and interoperable C2 capabilities and data links that support coordinated engagement decisions across distributed air-defence units, including in the presence of jamming, spoofing and cyber disruption.
- Decision support and automation tools for engagement planning and resource allocation that enable prioritised, timely and cost-aware responses to diverse threats, including UAS, loitering munitions and cruise missiles, under time-critical conditions.