NATO DIANA
Defence | Innovation | Adoption

2027 Challenge Statements

Table of Contents:

NATO DIANA
Defence | Innovation | Adoption

2027 Challenge: Human Survivability

Human Survivability

1. Challenge Summary: NATO operations increasingly place personnel in austere, contested environments where injury, physiological strain, environmental exposure, and cognitive degradation accumulate over time, often while specialist care and evacuation are delayed, constrained, or denied. In these conditions, survivability depends not only on treating discrete injuries, but on sustaining human performance and resilience under prolonged stress. Current approaches remain largely evacuation-centric and fragmented across protection, monitoring, care, and performance, creating critical gaps in the live-chain and continuum of care when medical capacity is disrupted, overwhelmed, or actively targeted. This opens an opportunity to shift toward more integrated, soldier-centric survivability and stabilisation concepts.

The Alliance seeks integrated, interoperable, and scalable solutions to protect individuals, mitigate threats, detect degradation early, and sustain human life and performance in contested and extreme environments. Emphasis is on maintaining force effectiveness when evacuation, resupply, and medical support are constrained or disrupted. Human survivability and the life-support chain must be treated as an operational system. Solutions must enable sustained, large-scale operations at high tempo while enhancing protection and situational awareness without increasing cognitive, physical, or logistical burden.

2. Illustrative Scenario: During a high intensity large-scale combat operation, dispersed NATO forces operate under persistent indirect fire, drone threat, electronic disruption, environmental stress, and uncertainty regarding chemical or biological exposure. Over time, personnel experience cumulative fatigue, dehydration, thermal stress, immune strain, and cognitive degradation, reducing decision quality, reaction time, and tolerance to injury. Following an engagement, multiple casualties occur due to blast and fragmentation, while environmental exposure and delayed treatment exacerbate survivability risks. Local and rear medical capacity is already exceeded due to the scale of operations, and evacuation is delayed for many hours due to contested airspace and dangerous ground routes. Integrated personal protection reduces secondary injuries and exposure. Wearable and environmental sensors detect blood loss, shock indicators, cognitive degradation, and early biological stress signals across the unit, enabling adaptive tasking and early intervention. Artificial Intelligence (AI)- guidance assists forward deployed stabilisation and prolonged field care, while hybrid crewed and uncrewed systems extract casualties under threat, with monitored in-transit care and digitised medical data supporting continuity of treatment.

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:

Adaptive Protection, Exposure Reduction, and Signature Management

- Lightweight, adaptive protection against ballistic, blast, chemical, biological, radiological and nuclear threats, directed-energy effects, and adverse weather, including thermal regulation and contamination resistance.
- Advanced camouflage and signature management reducing visual, thermal, acoustic, and electromagnetic detectability.

Prolonged Field-care, Casualty Extraction, and In-Transit Care

- Portable diagnostics, resuscitation tools, and point-of-need countermeasures for forward intervention, stabilization, treatment and prolonged field care.
- Technologies supporting autonomous or automated casualty and medical evacuation that reduce human overload, automate processes, and enable monitored in-transit care.
- AI-assisted triage, routing, and telemedicine support when specialists and evacuation assets are scarce.

Continuous Physiological, Cognitive, and Hazard Monitoring

- Multimodal biosensing for continuous assessment of vital signs, injury indicators, fatigue, and cognitive state.
- Monitoring of biological stress (e.g. immune or metabolic strain, early infection indicators) to anticipate degradation before injury.
- Pathogen (or synthetic entity) -agnostic detection of biological and chemical hazards for early warning and response.
- AI for converting sensor streams into actionable alerts and decision support.

Biotechnologies for Human Survivability and Scalable Operational Support

- Biological sensing and rapid diagnostics suitable for in-field deployment.
- Biotechnology-enabled countermeasures supporting protection, stabilisation, recovery, and sustainment under stress and injury.
- Biomanufacturing technologies for fuel, blood, protein, antibiotics, critical chemicals and high-energy materials.
- Scalable technologies for securing metabolic resilience in contested environments.

Human–Machine Teaming, Interfaces, and Interoperability

- Exoskeletons and dexterity augmentation to enhance mobility, casualty handling and surgery.
- Integrated soldier systems, including helmets with embedded sensing and communications.
- Augmented, virtual and mixed reality interfaces for training, tele-assistance, and real-time medical and operational support.
- Digitised medical documentation and patient tracking across the continuum of care.

NATO DIANA
Defence | Innovation | Adoption

2027 Challenge: Multidomain Autonomy of Uncrewed Systems

Multidomain Autonomy of Uncrewed Systems

1. Challenge Summary: Uncrewed systems today often operate as isolated platforms with limited autonomy, unreliable communications, and constrained ability to collaborate across air, land, maritime, and space domains, or to seamlessly share data. In contested environments, these shortcomings reduce the speed and reliability of sensing, decision-making, and effects, while increasing operator burden and susceptibility to disruption, deception, and attrition. Similar limitations also hinder civilian applications, such as disaster response, border monitoring, and critical-infrastructure protection. Emerging trends such as resilient autonomy, cooperative sensing, decentralised mission management, and predictive sustainment could enable multi-domain uncrewed vehicles to function as an integrated system that adapts in real time and remains effective despite interference and losses.

The Alliance seeks interoperable data-driven solutions that enable trusted, scalable, multi-domain autonomy and seamless integration of uncrewed and crewed platforms, allowing secure workflows and a data-rich tasking environment, based on consolidated command, control, communication, cybersecurity, computers, intelligence, surveillance and reconnaissance (C5ISR).

2. Illustrative Scenario: A large Allied port experiences a cyber-attack on vessel traffic control systems, global navigation satellite systems (GNSS), and communications. A multi-domain mix of autonomous uncrewed platforms—space, air, ground and maritime—is deployed, building up a data-rich common operational picture with integrated inference to uncover strategic adversary intentionality and likely next steps. Decentralised mission management guarantees coordination and orchestrated operations despite jamming, GNSS denial, spoofing, and intermittent connectivity, relying in part on innovative small satellites made from novel composites. Suddenly, a vessel carrying fertilizer spoofs loss of control authority, risking an explosive grounding. Further autonomous sensing nodes, featuring reduced electro-optic and infrared signatures as well as aspects of stealth, are dispatched. Integration with crewed response enables a rapid, effective, and de-risked threat curtailment. After onboard action, uncrewed platforms evacuate casualties, resupply materiel and carry out autonomous in-situ repairs. Similar capabilities are warranted in disaster response, border security, or organised-crime interdiction, as well as in direct military uses.

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:

Resilient Autonomy and Navigation

- Autonomous navigation to operate safely and effectively with degraded GNSS, uncertain maps and unknown terrain, dynamic obstacles across domains, and adversarial contestation.
- New subsystems and device components enabling autonomy to improve onboard perception, compute, timing, and power for low-size, weight and power (low-SWaP) autonomous platforms.
- New materials and design for manufacturing and signature reduction, to lower detectability and to enable survivability in multidomain contested and austere environments.

Multi-platform Orchestration and Cooperative Sensing

- Multiplatform orchestration methods to coordinate tasking, deconfliction, and effects delivery across heterogeneous assets.
- Co-operative sensing and decentralised build-up of the common operational picture to fuse distributed observations, resist deception, and maintain situational awareness under disruption.

Sustainment, Repair, and Scalable Production

- Predictive maintenance and in-situ autonomous repair to reduce downtime and logistics burden and sustain tempo under attrition and distance.
- Advanced, additive and adaptive manufacturing to enable rapid replacement, mission-tailored variants, and distributed production closer to the point of need.

Persistent, High-altitude and Space-enabled Support

- Structural power composite materials for high-altitude and space assets to extend endurance and enable persistent sensing and communications.
- In-orbit and in-air services to support servicing, replenishment, and extension of uncrewed capabilities in high-altitude and space environments.

NATO DIANA
Defence | Innovation | Adoption

2027 Challenge: Multidomain Sensing and Advanced Data Processing for Intelligence and Surveillance

Multidomain Sensing and Advanced Data Processing for Intelligence and Surveillance

1. Challenge Summary: The ability to detect, monitor, and observe activity across land, air, maritime, cyber, and space domains is critical to collective defence, security and resilience. Governments and operators increasingly rely on diverse sensing systems to support airspace management, infrastructure protection, environmental monitoring, crisis response, and situational awareness in complex operational environments.

In practice, sensing and surveillance are constrained by fragmented sensor networks, degraded or disrupted communications, and environments characterised by congestion, interference, deception, or concealment. Individual sensing systems often provide only partial or context-dependent insight. When data cannot be shared, combined, or assessed collectively, gaps in coverage, confidence, and persistence limit situational awareness and hinder the generation of a coherent Common Operational Picture (COP).

The Alliance seeks multidomain sensing and advanced data processing for intelligence and surveillance. It addresses solutions that improve how data is sensed, transferred, integrated, and exploited across heterogeneous sensors, systems, and domains, supporting reliable COP generation across organisations and nations. Relevant approaches may operate at the sensor edge, within distributed networks, or at fusion and decision support nodes.

2. Illustrative Scenario: An Allied country is responsible for monitoring activity in the airspace surrounding major cities, transport hubs, and critical infrastructure. During a major public event, a surge in uncoordinated drone detections is reported near civilian airports and energy facilities, coinciding with dense commercial air traffic and increased regional tension. Authorities must rapidly distinguish safety incidents from potential security threats while maintaining normal civilian operations.

Information is collected from a wide range of sources, including ground-based radars, passive radio frequency and infrared sensors, airborne platforms, satellites, and data shared by neighbouring nations and civilian authorities. Each sensing system provides valuable insight under specific conditions, but no single source offers sufficient coverage, confidence, or persistence on its own, particularly in congested or degraded environments.

By enabling data from multiple sensors, systems, and stakeholders to be shared, correlated, and assessed collectively, advanced sensing and data-processing solutions support the generation of a more reliable Common Operational Picture. This integrated view reduces false alarms, improves detection confidence, and enables timely, coordinated response and decision-making.

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:

Multidomain Sensing and Communications

- Multidomain and multi-sensor solutions that detect, track, and monitor objects, activities, or anomalies across land, air, maritime, cyber, and space domains.
- Secure, resilient, and adaptive communications technologies that enable intelligence and surveillance data sharing across contested, congested, or degraded electromagnetic and cyber environments.
- Novel sensing approaches, including passive, distributed, or emerging sensing modalities, that improve detection, persistence, and survivability under interference or adversary countermeasures.
- Applications relevant to Earth observation, airborne and maritime surveillance, electromagnetic and cyber sensing, and space-based monitoring, including capabilities associated with signals intelligence, imagery intelligence, communications intelligence, space situational awareness, and space domain awareness.

Advanced Data Processing and Fusion

- Artificial intelligence enabled analytics to filter noise, correlate heterogeneous data, detect patterns, and support tracking, classification, and assessment across large scale intelligence and surveillance data sets.
- Edge and distributed computing technologies that allow data to be processed close to the sensor or user, reducing latency and dependence on centralised infrastructure.
- Data management, labelling, and metadata solutions that improve interoperability, trust, discoverability, and reuse of intelligence and surveillance data across systems and nations.

Intelligence and Surveillance Decision Support

- Tools that support intelligence analysis, prioritisation, alerting, and assessment to inform decision-making across echelons.
- Data-centric architectures that enable flexible integration of sensing and intelligence outputs into command-and-control systems.
- Cross-domain cueing and correlation solutions that allow information collected in one domain to enhance intelligence and surveillance in another.

NATO DIANA
Defence | Innovation | Adoption

2027 Challenge: Operational Resilience in Contested Environments

Operational Resilience in Contested Environments

1. Challenge Summary: In contested environments, adversaries deliberately disrupt sensing, communications, and navigation through cyber-attacks, electromagnetic spectrum interference, and the denial of global navigation satellite systems (GNSS). Combined with austere and extreme physical conditions, these actions constrain freedom of action by limiting mobility, slowing decision-making, and restricting command-and-control (C2). As a result, both military operations and other vital security functions, such as the protection of critical infrastructure, are exposed to heightened risk.

The Alliance seeks practical, interoperable sensing, communication and positioning, navigation, and timing solutions that maintain operational effectiveness at the tactical edge when connectivity and assured navigation cannot be assumed. Solutions should enable coordination, safe movement and situational awareness and be inherently resilient to spectrum contestation and GNSS denial when deployed across mixed and austere terrain. This includes the detection and classification of adversary communications and assets whilst protecting friendly ones. Together, such capabilities would enhance operational resilience, freedom of action and continuity of operations.

2. Illustrative Scenario: An Allied response force is deployed to a partner nation after disruption to a regional airport and energy infrastructure. Visibility is degraded and the electromagnetic environment is subject to adversary jamming, further compounded by friendly countermeasures. Conventional radios prove unreliable and GNSS access is actively denied, limiting C2 and freedom of manoeuvre.

A forward unit deploys an uncrewed aerial system to perform reconnaissance on potential threats. Using GNSS-independent navigation and a multi-spectral sensing package, this detects an unmarked convoy approaching restricted airport access roads despite visual obscuration. Information is relayed using a resilient mesh radio network that dynamically routes data across tactical, satellite and civilian 5G data links. By correlating this information with high-definition satellite imagery from a civilian provider and analysis of electromagnetic emissions, the unknown convoy is identified as adversary. An unmanned ground vehicle, fitted with an electromagnetic-signature-reducing-coating, is then deployed to perform further reconnaissance under cover of darkness. Throughout the operation, the unit maintains coordination and safe movement across varied and austere terrain without reliance on assured access to the electromagnetic spectrum.

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:

Spectrum Management

- Methods for monitoring spectrum availability, including the detection of low-interference and under-utilised bands.
- Solutions for detecting and characterising electromagnetic radiation, including weak, intermittent and low-probability-of-intercept emissions.
- Artificial intelligence (AI)-enabled approaches to dynamic spectrum management in congested electromagnetic environments.

Resilient Communication Systems

- Low-probability-of-intercept data links, for example using millimetre and terahertz radiation, that maintain reliable communications in contested environments.
- High-bandwidth, interference-resistant terrestrial and space-based communication systems that sustain connectivity when conventional radio-frequency links are degraded or unavailable.
- Self-configuring and autonomously deployable mesh networking technologies that provide resilient communications without reliance on fixed infrastructure.

Adaptive Sensing Technologies

- Software-defined systems using cognitive features, such as AI-enabled spectrum awareness and channel deconfliction, to adapt to evolving conditions.
- Integrated sensing and communications approaches for efficient spectrum usage with minimised hardware complexity and electromagnetic footprint.
- High-sensitivity sensing technologies, including quantum-enabled solutions, for measuring weak signals and detection and ranging with reduced probability of interception under contested conditions.

Resilient Navigation, Positioning and Timing

- Inertial measurement units, magnetic sensors and vision-based approaches using terrain and celestial observations that enable accurate navigation without relying on external signals.
- Alternatives to GNSS such as navigation systems utilising low Earth orbit satellites or radio-frequency signals of opportunity.
- Resilient timing and synchronisation solutions that enable the distribution of trusted time references in GNSS-denied environments.

Protection and Mobility

- Advanced materials and surface treatments that enable electromagnetic signature reduction, including frequency-selective surfaces and metamaterials.
- Platform protection and mobility-enabling approaches that reduce detectability and support movement in visually degraded and denied environments.

- Portable systems for collecting signals and imagery intelligence, such as edge sensors equipped with wideband receivers and embedded AI, for identifying adversary emissions amongst background noise.

NATO DIANA
Defence | Innovation | Adoption

2027 Challenge: Responsive Logistics

Responsive Logistics

1. Challenge Summary: Modern civilian and defence systems alike rely on resilient logistics and agile mobility, creating a strong demand for dual-use solutions that can enhance supply-chain resilience and infrastructure robustness. The ability to move, sustain, and support people, equipment, and data across complex, distributed, and often degraded environments is essential for mission safety and operational success. Solutions that improve efficiency, resilience, and adaptability in civilian contexts can also strengthen defence readiness in crisis or conflict. Disruptions caused by extreme weather, infrastructure degradation, cyber interference, or contested access can rapidly expose the fragility of long, linear supply chains and labour-intensive processes.

Meeting these challenges depends on multi-domain redundancies and advanced in-situ repair and maintenance capabilities. Additionally, predictive maintenance, digital twin-based diagnostics, additive manufacturing, and autonomous delivery will be required across all domains, including space. The Alliance seeks smart, interoperable logistic mobility solutions that sustain endurance and freedom of action in dynamic environments, strengthening collective defence and security.

2. Illustrative Scenario: A NATO-led multinational task force deploys at short notice to a remote, infrastructure-poor region following a rapidly escalating crisis near a contested border, requiring simultaneous humanitarian and military operations. As forces are deployed, interoperable predictive logistics and communications systems enable Allies to coordinate movement, intelligence, surveillance and reconnaissance (ISR), supply distribution, personnel recovery and humanitarian action. Dynamic multi-domain logistics systems enable real-time reallocation of materiel, food, medical supplies, and mobility assets in response to evolving humanitarian needs, weather, terrain, and security conditions. A shared digital logistics picture enables prioritised real-time resupply, mobilisation of ad-hoc logistics hubs, means and routes, rapid cross-border convoy clearance and dynamic route adaptation even in the face of intensive forward operations. When equipment fails within dispersed maintenance areas, mobile repair teams employ autonomous diagnostics, digital twins and additive manufacturing to restore essential civilian and military capabilities within hours, sustaining operational tempo and combat effectiveness.

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:

Resilient Mobility & Responsive Logistics under Contested Conditions

- Autonomous logistics planning and optimisation platforms to strengthen end-to-end supply chain resilience, redundancy, and sustainment across contested and disrupted environments.
- Artificial intelligence (AI)-enabled stock allocation and demand forecasting to support time-critical decisions and balance military and civilian needs.
- Interoperable logistics command-and-control (C2) software enabling multinational coordination, digitised cross-border movement, materiel substitution and interoperability.
- Data fusion capabilities generating a shared logistics picture to support coordinated sustainment decisions across domains.

Rapid Sustainment, Predictive Maintenance & Lifecycle Resilience

- Operational digital twins for vehicles, systems, and sensors to enable rapid in-field repairs.
- AI-based fault diagnosis and simulation-driven assessment tools that operate under incomplete or degraded data conditions to support partial repair and functional bypass when spares, tools, or access are limited.
- Additive manufacturing and repair by addition toolchains, including in-space servicing, assembly, and manufacturing, to restore critical components without reliance on deep logistics hubs.
- Software recalibration and system reconfiguration tools to improve interoperability and ad-hoc integration of equipment and systems.

Energy Resilience

- Deployable renewable power generation and tactical energy storage to support expeditionary and contested operations, including space-dependent missions.
- AI-enabled energy and power management systems, including edge-AI control electronics, to maintain resilience against degradation, wear, or kinetic effects.
- Energy saving and energy harvesting technologies to reduce dependence on fixed supply routes and logistics tails.

Mobility Platforms & Secure Transport

- Low-signature, stealth and protected mobility vehicles adapted from civilian technologies to offset bespoke platform shortages.
- Packaging and storage systems that are resistant to shock, vibration and extreme environments.
- Modular vehicle architectures supporting ISR, C2, logistics, and casualty evacuation.
- Delivery, autonomous resupply, and rendezvous and proximity operations solutions to shorten logistics tails and reduce personnel risk across domains.

NATO DIANA
Defence | Innovation | Adoption

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.