Immersive infrastructure as a strategic capability in defense

Immersive infrastructure as a strategic capability in defense Virtual reality (VR) and mixed reality (MR) have become firmly established in military training.

However, their true value lies not so much in the quality of the simulation, but in the infrastructure that makes it viable, scalable, and manageable.

In the defense sector, immersive training involves critical platforms integrated into existing infrastructure, aligned with security policies, and designed to evolve over decades. More than just simulators, they are structural systems that support distributed training, collaboration between units, and continuous adaptation to changing scenarios.

Among its benefits are: safe training, the ability to repeat complex maneuvers, the simulation of situations that are difficult to recreate, and multi-location collaborative training. In addition, they improve efficiency by reducing the use of physical resources and accelerating learning cycles.

However, the environment imposes key requirements: segmented networks, data sovereignty requirements, classified environments, or even air-gapped environments.

Therefore, the infrastructure must support synchronized multi-user operations, zero-trust models, centralized identity management, and offline modes.

A suitable platform—such as VIROO — It enables the centralization of content, ensures operational consistency and traceability, and integrates with corporate systems in a secure and governed manner. Without this infrastructure layer, scaling immersive training increases operational and technological risks.

Equally critical is the autonomy and ability to create and update content. Enabling in-house development based on common standards reduces dependencies, streamlines doctrinal adaptation, and strengthens technological sovereignty.

In this way, immersive training ceases to be an isolated project and becomes integrated into the organization's overall set of digital systems and processes (digital thread), evolving into a structural capability that is sustained over time.

From an economic and strategic perspective, this infrastructure protects investments, reduces vendor lock-in, and supports the long lifecycles typical in the defense sector. Finally, it must be deployment-agnostic: cloud, private, on-premises, or isolated environments.

This flexibility ensures regulatory compliance and full control over the data.

→ Read the full article on XR infrastructure

This approach will be one of the main focuses of Virtualware's presence at Eurosatory 2026 (Paris, June 15–19), one of the leading international events in the defense and security sector.

At the Spanish Pavilion, organized by TEDAE, the company will demonstrate how its VIROO platform enables the deployment, management, and scaling of collaborative training and simulation environments in a centralized, secure, and multi-user manner. It will present one of its use cases, SIMUR, an advanced VR training simulator developed in collaboration with the Military School of Health (EMISAN), designed for training in CBRN scenarios using protocols aligned with NATO standards.

This system has been showcased at technical forums and international industry events.

Virtualware's participation in Eurosatory reinforces its position as a technology partner in the defense sector, following years of collaboration with the Ministry of Defense, its involvement in NATO projects, and its integration into TEDAE, driving the adoption of immersive and 3D technologies in complex operational environments.

VR and MR are already established capabilities whose sustainability depends on infrastructure. In the defense sector, this is not about a one-off technology, but rather a strategic foundation that enables better training, reduces risks, and ensures long-term control—a vision that Virtualware is bringing to this year's Eurosatory 2026

→ Read the full article on XR infrastructure in defense