White Paper

A tense European defense context demands digital renovation of European armed forces

NetApp
November 2025

Summary

European defense forces are accelerating digital transformation to maintain operational superiority amid rising geopolitical and cyber threats. This evolution focuses on three strategic priorities: cloud adoption for agility, AI integration for enhanced decision-making, and robust cybersecurity to counter sophisticated attacks. Building resilient, interoperable data infrastructures and secure operating environments is essential to support multi-domain operations and ensure mission readiness. These initiatives aim to strengthen sovereignty, improve collaboration, and enable faster, data-driven responses in an increasingly complex defense landscape.

TABLE OF CONTENTS

Introduction

In a high-intensity European geopolitical context, where data management is becoming increasingly crucial, the defense sector must accelerate its digital transformation. This transformation revolves around three key priorities: broader adoption of cloud technologies, more refined use of AI, and enhanced cybersecurity responses. European armed forces face numerous challenges both in their daily operations and in the field. With its recognized expertise in data management services, NetApp supports them in this technological transition.

A tense European defense context demands digital renovation of armed forces

The war in Ukraine has brought back high-intensity conflict and highlighted the urgent need for adaptation and innovation in the face of hybrid warfare—combining direct combat with indirect actions like cyberattacks and information manipulation. This has led the EU to strengthen its defense capabilities, including through the **EDIRPA program** (adopted in October 2023), which encourages joint responses to critical defense needs among member states. With a budget of €310 million, EDIRPA facilitates cooperation and simplifies joint procurement processes.

In November 2024, the European Commission approved funding for five cross-border projects, including joint acquisition of air defense systems and ammunition stockpiles. This marks a new phase in European defense, emphasizing the need for resilient, robust, and agile IT infrastructures.

Countries like France and Germany are leading this digital renovation. France's **Military Programming Law (2024–2030)** aims to strengthen AI integration, secure application hosting for field operations, and modernize digital services. Germany has elevated its **Cyber and Information Domain Service (CIDS)** to the same level as its traditional military branches, reflecting the growing importance of information warfare and technological innovation.

NetApp: A Trusted Partner for Armed Forces

NetApp specializes in intelligent data infrastructures, offering unified storage, strong data security, integrated services, and CloudOps solutions. NetApp helps defense organizations tackle three major data challenges:

1. Data sprawl across on-premises and cloud environments: NetApp simplifies management.
2. Constant threats: NetApp ensures security and reliability.
3. Data movement and placements limitations: NetApp provides agility and cost-effective data placement.

The movement toward data operating centers to better serve armed forces

Despite ongoing digital transformation, challenges remain—especially in data management, which is now seen as a strategic resource. The defense sector produces and consumes vast amounts of data but struggles with usage and exploitation due to the need to connect highly protected data with less secure networks. Examples include:

- **Weapon systems**: Who owns the technical data collected from systems maintained by external manufacturers?
- **Open-source intelligence (OSINT)**: How can teams maintain analytical capabilities when AI is used maliciously to manipulate public opinion?

To address these challenges, defense IT systems must shift from on-premises models to cloud-based architectures. Field operations could benefit from “combat clouds” that enable secure, fast, and easy data sharing among deployed units.

Institutions like France’s **Defense Digital Commissariat (CND)** and Germany’s **CIDS** are working toward establishing **data operating centers** to support multi-domain operations with end-to-end connectivity to support everything from reconnaissance drones to soldiers on the ground.

Cloud, AI, and cybersecurity: The triple-digit challenge for armed forces

More cloud for better data agility

The defense sector must transition from centralized IT models to cloud environments. This “move to cloud” offers automation, enhanced security, and operational flexibility. NetApp supports this migration, notably in France’s Ministry of Armed Forces, using **NetApp® ONTAP® data management software**, which optimizes data lifecycle management in shared environments.

The ONTAP dashboard and unified storage layer allow administrators and users to monitor and enhance data exchanges. It supports cloud migration without modifying mission-critical application code, making it ideal for defense use cases.

More AI for operational efficiency

Since the Ukraine conflict began in 2022, European armed forces have seen increased drone usage and cyber warfare. AI plays a central role in intelligence and advanced weapon systems like coordinated drone swarms.

France’s **AMIAD (Defense AI Agency)** and Germany’s strengthened **CIDS** reflect AI’s growing military importance. AMIAD has a €300 million budget and aims to recruit 300 top-tier experts by 2026. Projects include acoustic data processing for submarine operators and faster identification of vehicle parts. AI helps operators make decisions in urgent or data-heavy situations—requiring secure, high-performance data environments, where NetApp excels.

More cybersecurity to counter sophisticated threats

Cyberthreats in defense include **espionage**, **sabotage (including ransomware)**, and **subversion**. Sabotage has become industrialized, often involving organized crime or state actors.

Attacks increasingly target **semantic layers**—spreading misinformation, propaganda, and manipulated media. Defense must adopt **DCS (data-centric security)** and **Zero Trust** approaches. NetApp’s ONTAP system offers native cyber resilience features, including rapid and secure backup and replication plans.

Learn more

Contact us today to explore how we can support your goals with proven, defense-grade, secure solutions that deliver clarity, resilience, and a strategic edge.

Contact a NetApp defense specialist

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp