OPCP

On-Prem Cloud Platform

Defend. Act. Control.

Operational superiority relies as much on expertise in digital technology as on military power.

Digital infrastructures are becoming a key strategic asset.

Defence: ensuring a nation's freedom of action.

Defence is the foundation of national sovereignty.

It ensures national defence, population safety, stable institutions, a country's ability to make strategic decisions without external interference.

The armed forces (land, air, maritime, cyber, space, or intelligence) operate in an environment characterised by:

- **the rise of hybrid threats** (cyber, information, satellite, technological pressures),
- **the escalating pace of conflicts** and the shortening of decision-making cycles,
- **the increasing volume of data** required for command and intelligence,
- **the digitisation of operations**, from strategic planning to the tactical execution,
- **critical dependence** on persistent, secure, and interoperable digital systems,
- **digital technology's ever-larger role in** defence platforms, hardware, and manufacturing processes.

In this context, military power also hinges on conventional weapon systems and **deep expertise in information**, algorithms, networks, and digital infrastructures, from industrial design to deployment.

A nation's self-defence capabilities are therefore contingent upon its **digital resilience, technological sovereignty, the output of its defence sector, and its armed forces'** capacity for sustained operations, even in the face of disruption or conflict.

Digital technology in defence: a force multiplier

Modern warfare depends fundamentally on technology, and that dependence is sustained by a symbiotic relationship between the military and defence manufacturers.
The industry's role involves designing, integrating, and maintaining the digital components essential for weapon systems and key military platforms:

Command, control, Communications, and Computers (C4)

Headquarters and command posts require consolidated, up-to-the-minute, reliable, and actionable information to effectively plan, coordinate, and execute operations—from initial capability design to deployment in the field.

Intelligence, Surveillance, and Reconnaissance (ISR)

Imagery, interception, ground, naval, aerial, and space-based sensors, along with ISR systems on platforms, generate massive amounts of data. This data must be collected, processed, and utilised locally, including in embedded or disconnected environments.

Cyber defence and cyber-offensive

Supervision centres, cyber units, and industries responsible for critical architectures must be prepared to analyse, detect, respond to, and counter sophisticated state-sponsored attacks. This approach protects both operational systems, industrial supply chains, and deployed platforms.

Simulation, preparation, and training

Forces and industries rely on immersive virtual environments, digital twins and intensive computing capabilities to design systems, plan operations, train personnel, and confirm real-world scenarios.

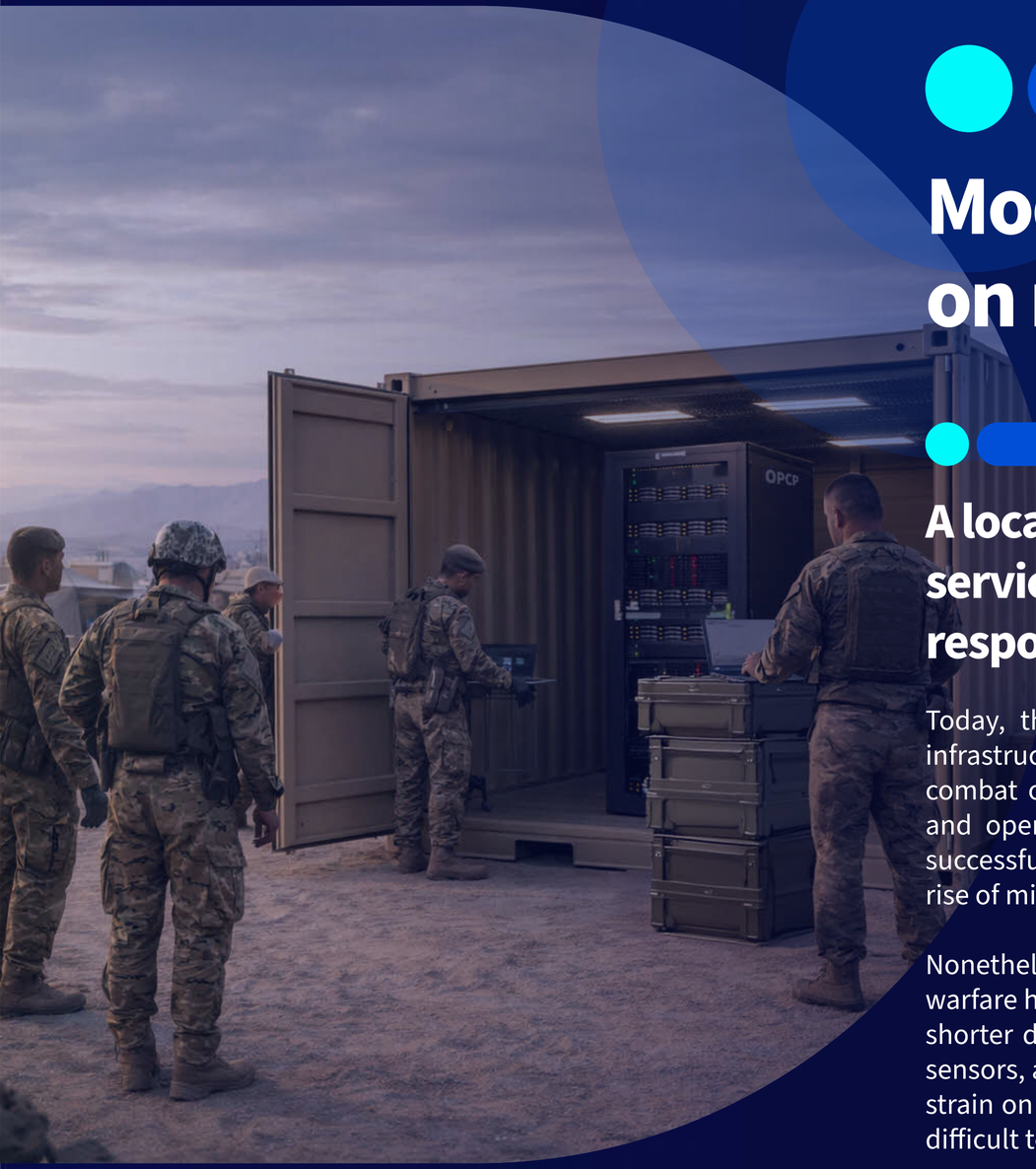
Logistics and in-service support (ISS)

Uninterrupted digital links between deployed units, rear-area bases, and defence manufacturers are crucial to resource tracking, predictive equipment upkeep, fuel management, munitions, and spare parts.

AI in the military and its role in decision-making

AI models for defence applications, like predictive analysis, anomaly detection, electronic warfare, and force protection, need secure, on-site infrastructure that can operate in restricted or embedded environments.

These uses demand **a digital backbone stretching from senior command posts to the tactical field**, and even to industrial or embedded systems, offering automation, resilience, and security capabilities far exceeding those of conventional architectures.



Modern warfare calls for a new perspective on military strength.

A locally delivered public service with a high level of responsibility.

Today, the armed forces are equipped with digital infrastructures that are robust enough to handle combat operations, leadership, intelligence, logistics, and operational upkeep. These infrastructures have successfully served their purpose and supported the rise of military digital technology.

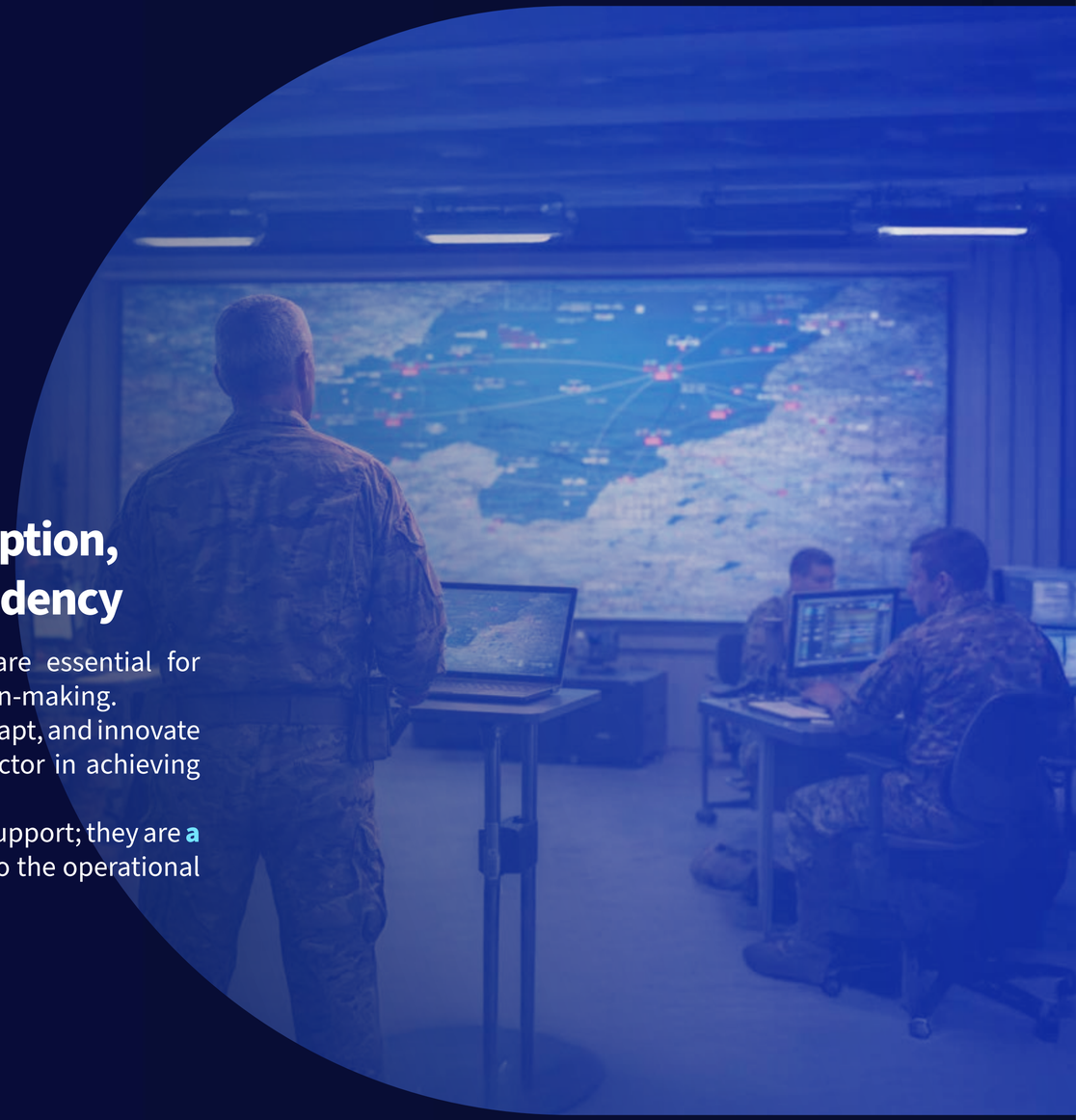
Nonetheless, the dynamics and nature of modern warfare have dramatically changed. Escalating threats, shorter decision-making cycles, a growing number of sensors, and exponential data growth place significant strain on architectures that are often rigid, siloed, and difficult to update.

A disruptive operational environment

Forces must now operate in hybrid, disputed, and volatile environments where digital continuity, complete local autonomy, and resilience are no longer options but fundamental necessities. The pressure on older infrastructures is immense as they are required to simultaneously support AI integration, real-time processing, tactical mobility, and enhanced security against technologically advanced state adversaries.

Within this context, improving existing infrastructures is key to consolidating and extending military advantage.

Maintaining military strength with digital infrastructure assets.



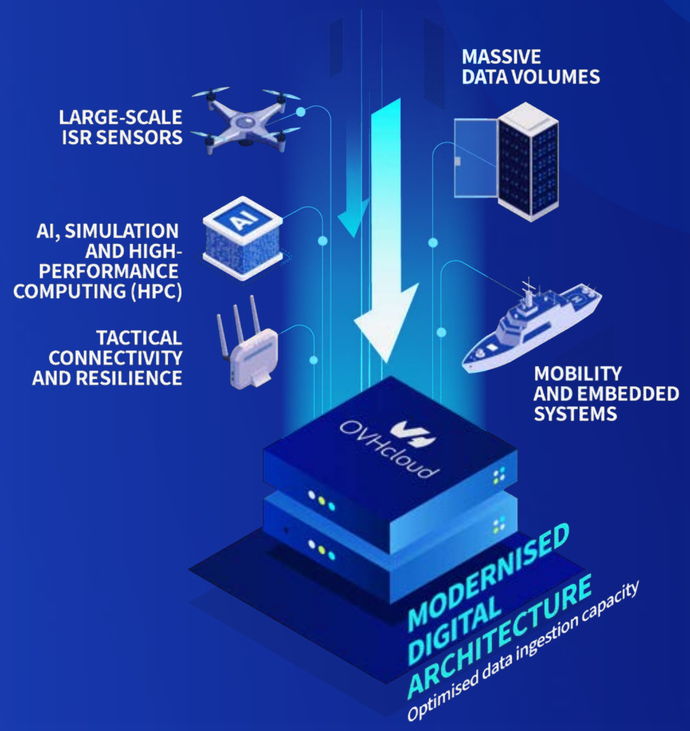
Going beyond basic maintenance

To stay ahead, it is crucial to build infrastructure that can continuously adapt to changing operational demands, rather than relying on occasional system updates. The real challenge is turning a robust digital foundation into a tool for long-lasting competitive advantage, allowing for rapid integration of new capabilities without disrupting ongoing operations.

This highlights the need for an infrastructure that can flexibly incorporate innovations such as AI, automation, or advanced data mining—while maintaining complete control, sovereignty, and security.

Innovating without disruption, operating without dependency

Steady, measured military innovations are essential for supporting tactical movement and decision-making.
In modern warfare, the ability to outlast, adapt, and innovate faster than the opposing force is a key factor in achieving military dominance.
Digital infrastructures are no longer just a support; they are **a full-fledged military capability**, central to the operational freedom of the armed forces.



A vital digital transformation: outdated systems as a strategic risk.

Current digital infrastructures for the military and defence sector, built for operational and industrial needs, are no longer adequate. They are:

- distributed across the armed forces, programmes, and industrial players,
- diverse in their technologies and maturity levels,
- outdated and difficult to modernise,
- poorly suited to rapid deployments or embedded environments,
- often incompatible, even with systems built for interoperability,
- costly to maintain over life cycles that extend for many decades.

These architectures struggle to absorb:

- the significant increase in ISR sensors deployed across platforms and combat zones,
- the growing computational needs for AI, simulation, and advanced analysis,
- tactical connectivity and resilience requirements in disputed environments,
- the exponential volumes of strategic and industrial data.

The risk to **military and industrial continuity is substantial**, as these infrastructures are no longer suited to evolving uses and demands. This curtails operational agility, prolongs decision-making cycles, makes coordinating joint and cross-programme initiatives more difficult, hinders the scalability of platforms, and exposes forces to serious vulnerabilities.

To put it another way, digital modernisation is more than just an IT project, **it is a fundamental requirement for operational advantage, industrial consistency, and lasting sovereignty.**

The modern on-site cloud for defence: a cloud that adapts to combat zones.

Un cloud militaire de nouvelle génération doit offrir des capacités que les plateformes traditionnelles ne fournissent pas, afin de soutenir à la fois les opérations, les plateformes embarquées et les environnements industriels critiques :

Quick deployment
Automated setup of a fully functional environment in minutes, suitable for command posts, advanced bases, embedded platforms, or sensitive manufacturing locations.

On-site operations
Local and autonomous capabilities for advanced bases, vessels, deployed detachments, and tactical command centres, as well as for platforms and industrial workshops operating in limited environments.

Full air-gapped mode
Systems without network dependencies or mandatory interconnectivity, enabling continuous operation in complete isolation, whether in combat zones, aboard strategic vessels, or within classified production locations.

Advanced automation
Standardised, reliable, and largely automated operations, even in reduced capacity environments, mostly automated to lessen CIS units and industrial teams.

Tactical computing
Ultra-low latency for embedded AI, drones, radars, optronic systems, and sensors integrated into platforms, with computing capabilities deployed as close as possible to weapon systems.

Enhanced protection
Military-grade cyber hardening, incorporating advanced protection mechanisms for operational, industrial, and embedded environments.

Controlled interoperability
Ability to interface with external clouds or partner systems when necessary, without structural dependencies or loss of sovereignty.

The operational and industrial might of modern militaries is significantly boosted by this cloud technology, positioning it as central to their power.

OPCP: a cloud platform built for Defence, covering strategic and tactical needs.

Designed as a cloud-native on-premises platform, OPCP can be deployed in these environments:

- → Defence datacentres,
- → Defence industries,
- → classified IT sites,
- → tactical operation centres,
- → vessels,
- → deployed bases,
- → conflict zones,
- → disconnected environments.

It offers:

- → automated deployment,
- → hardening-ready military infrastructure,
- → joint military IT governance,
- → digital resilience,
- → total autonomy in isolated mode,
- → service orchestration.

OPCP provides Defence with a unified architecture, designed for both military and industrial use, and equipped to support the long-term growth of AI, cyber, and modern C4ISR.

LANDING ZONE MANAGER

Governance:

- → strict isolation by unit, mission, or project,
- → classification policies,
- → advanced access control,
- → national or local oversight.

CLOUD STORE

The military catalogue:

- → C4ISR applications,
- → tactical AI engines,
- → analytical environments,
- → rapidly deployable services, including in air-gapped mode.

OPCP CORE

A secure foundation:

- → compute/network/security orchestration,
- → automated patching,
- → multi-level resilience,
- → autonomy in isolated sites,
- → complete observability for command posts.

On-premises cloud as a military force multiplier.

As illustrated by the provided use cases, a next-generation cloud infrastructure, such as OPCP, meets the specific requirements of the Defence ecosystem at all levels: strategic, tactical, and industrial.

They demonstrate the cloud's role in multiplying military strength through enhanced **resilience, faster decision-making, and the sustainable growth of operational capabilities in all military and industrial contexts.**

OPCP

USE CASE | **01**

Deployable and resilient digital command posts.

Modern operations move at a fast pace, so command posts (CP) must be able to:

- → **deploy quickly,**
- → **be operational in minutes,**
- → **be resilient to attacks,**
- → **operate independently of external networks,**
- → **be interoperable with allied units.**

In the chaos of disputed environments, the C4ISR chain requires resilience against jamming, satellite disruption, or cyber pressures.

OPCP provides:

- → **fully automated** service deployment, intelligence, planning, and operational monitoring,
- → an **architecture engineered to operate autonomously**, without connection torear command posts,
- → a **multi-level resilience**: local failover, instant recovery, and security primitives that enable the setup of integrated cyber hardening,
- → the **capability to locally run** critical applications,
- → **stable performance** even in extreme conditions (climate, transport, high-intensity operations).

The CP becomes a fully digital, mobile, robust, and self-sufficient nerve centre, able to maintain its advantage, even with disrupted communication channels.

OPCP

USE CASE | **02**

Sovereign use of military AI and ISR.

Modern intelligence, characterised by its massive volume, wide variety, and rapid pace, demands secure processing right at the source: IMINT, SIGINT, HUMINT, OSINT, ROEM, radars, satellites, tactical drones, and electronic warfare.

The armed forces must be able to:

- **ingest, integrate**, and analyse data streams from multiple sources,
- train and deploy **military AI models** on-site,
- ensure **immediate** processing, even without a global network,
- protect **classified data** at Secret or Top Secret level.

OPCP ensures:

- **sovereign processing** of critical data, without transfer to an external provider,
- the **inference of AI models** directly in combat zones,
- the management of **automated ISR pipe lines**: from ingestion through correlation and analysis to decision-making,
- a **fully air-gapped** operation, eliminating any risk of leakage,
- **controlled dissemination** across strategic, operational, and tactical levels.

The intelligence-decision-action loop is accelerated, made secure, and independent of sovereignty or communication constraints.

OPCP

USE CASE | **03**

Tactical cloud for deployed units

Embedded digital systems, sometimes deployed for several months in isolated environments (without reliable connection), are required to keep running and processing critical data. They are designed to support operational continuity, even when external communications are impaired or severed.

To achieve this, deployed units need a compact, hardened, and independent cloud, one that requires **minimal logistical requirements.**

On-site processing is needed for operations in the following areas:

- → embedded AI (detection, classification, trajectory),
- → sensor data stream processing,
- → tactical combat,
- → communications and information exchange management.

OPCP delivers:

- → a **robust tactical cloud**, able to operate in a mobile CP, fleet vessel, or advance detachment,
- → **low-latency local processing** enabled by tactical proximity to weapon systems,
- → **delayed synchronisation** in case of reconnection, without data loss,
- → **automation** that minimises the need for expert personnel,
- → **total service continuity** even when mobile or disconnected.

Forces gain autonomy, make decisions faster, and benefit from better information access.

OPCP

USE CASE | **04**

National resilience during crises and cyberattacks.

A completely isolated and independent cloud.

State-sponsored cyberattacks targeting national infrastructure can paralyse:
- → communications,
- → logistics,
- → financial systems,
- → command posts,
- → alerting systems,
- → military bases.

The armed forces must ensure operational capability, **even if national digital systems temporarily fail.**

OPCP ensures:
- → the **operational upkeep of critical applications** (military health, fuel, munitions, HR, C4ISR),
- → **rapid recovery** following a breach of the primary system,
- → **zone-specific resilience**, where each site can operate as a sovereign enclave,
- → the **potential for enhancing cybersecurity** that aligns with military and national security agency protocols,
- → **immediate isolation** of a breached location without disrupting other areas.

The State is therefore equipped to maintain its defences, direct its armed forces, and coordinate its resources, even during a large-scale cyberattack.

OPCP

USE CASE | **05**

Joint/allied pooling and interoperability.

Modern military operations span multiple areas and rely on:
- the Army,
- the Air and Space Force,
- the Navy,
- Cyber defence units,
- Intelligence,
- various alliances (NATO, bilateral partnerships, UN missions).

IT systems must therefore be:
- consistent and aligned,
- technologically compatible,
- segmented based on classification levels,
- supervised consistently.

OPCP delivers:
- a **unified foundation** for the armed forces and agencies of the Ministry of Defence,
- **strict** perimeter **isolation** (units, mission, projects),
- **security policies tailored** to classification levels (Secret to Top Secret),
- **standardised deployments**, minimising costs and risks,
- a **secure way to collaborate** with allied forces.

As a result, Defence achieves greater unity, streamlined processes, and enhanced capability to conduct joint operations.

OPCP

USE CASE | **06**

Industrial sovereign cloud for the design, in-service support, and upgrade of weapon systems.

The defence industry is responsible for managing critical weapon systems and platforms that are designed for long-term operation, requiring digital infrastructures that can:

- support long and complex life cycles,
- process sensitive and classified data,
- support the ongoing expansion of capabilities,
- ensure seamless transition from design through production to operation,
- maintain control over data and models.

It is therefore important to ensure the security and consistency of these industrial digital environments, while allowing for a regulated flow of information to the armed forces, without external exposure or reliance.

OPCP provides:

- an **on-site, sovereign industrial cloud**, used for design, simulation, testing, and in-service support (ISS).
- **support for digital twins**, large-scale simulations, and AI computing for critical data,
- **digital continuity** between defence manufacturers, government bodies, and the armed forces, all with clearly defined operational boundaries,
- the **capability to deploy secure working environments** on industrial sites, support bases, or maintenance centres,
- a **gradual modernisation of industrial digital systems** without disrupting existing programmes.

The defence industry thus benefits from a unified, sovereign, and sustainable digital foundation, ensuring the availability, growth, and performance of military capabilities over time.

A pairing with purpose

Proven technical solution, combined with industry-specific expertise.
Clearly, there are things we need to do together.

Cases to develop, adapt and test

There’s no shortage of use cases: edge, factories, critical sites, disconnected infrastructure, and much more. What if we focused on one or two key areas to make real progress?

A workshop, a chat, a POC?

We don’t need to put everything on hold just yet.
Let’s brainstorm, see which ideas make sense, and gradually build.

ovhcloud.com
opcp@ovhcloud.com