OPCP

On-Prem Cloud Platform

Défendre. Agir. Dominer.

La supériorité opérationnelle repose autant sur la maîtrise du numérique que sur la puissance militaire.

Les infrastructures numériques deviennent un atout stratégique essentiel.

La Défense : garantir la liberté d'action d'une Nation.

La Défense constitue le socle de la souveraineté nationale.

Elle assure la protection du territoire, la sécurité des populations, la stabilité institutionnelle et la capacité d'un pays à exercer ses choix stratégiques, sans contrainte extérieure.

Les forces armées qu'elles soient terrestres, aériennes, navales, cyber, spatiales ou de renseignement, opèrent dans un environnement marqué par :

- **la multiplication des menaces hybrides** (cyber, informationnelles, satellitaires, pressions technologiques),
- **la vitesse croissante des conflits** et la réduction des cycles décisionnels,
- **l'explosion des volumes de données** nécessaires au commandement et au renseignement,
- **la numérisation des opérations**, du niveau stratégique jusqu'au niveau tactique,
- **la dépendance critique à des systèmes numériques** continus, sécurisés et interopérables,
- et **l'intégration croissante du numérique** au cœur des plateformes, des équipements et des chaînes industrielles de défense.

Dans ce contexte, la supériorité militaire dépend désormais autant des systèmes d'armes classiques que de **la maîtrise de l'information**, des algorithmes, des réseaux et des infrastructures numériques, depuis la conception industrielle jusqu'à l'emploi opérationnel.

La capacité d'un pays à se défendre repose donc sur sa **résilience numérique,** sa **souveraineté technologique, la performance de son industrie de défense et la capacité de ses forces armées** à opérer durablement, y compris en environnement contesté ou dégradé.

Le numérique de Défense : un multiplicateur de puissance

Les opérations militaires contemporaines reposent sur un socle technologique devenu central, partagé entre les forces armées et l'industrie de défense, qui conçoit, intègre et maintient les capacités numériques au cœur des systèmes d'armes et des plateformes critiques :

Commandement et contrôle (C4)

Les états-majors et centres de commandement doivent disposer d'une information consolidée, en temps réel, fiable et exploitable pour planifier, coordonner et conduire les opérations, depuis les phases de conception capacitaire jusqu'à l'emploi opérationnel sur le terrain.

Renseignement multi-sources (ISR)

L'imagerie, l'interception, les senseurs terrestres, navals, aériens et spatiaux, ainsi que les systèmes ISR intégrés aux plateformes, produisent des volumes massifs de données qui doivent être collectées, traitées et exploitées localement, y compris en environnement embarqué ou isolé.

Cyberdéfense et cyber-offensive

Les centres de supervision, les unités cyber et les industriels en charge des architectures critiques doivent analyser, détecter, réagir et opérer face à des attaques étatiques sophistiquées, en protégeant aussi bien les systèmes opérationnels que les chaînes industrielles et les plateformes déployées.

Simulation, préparation et entraînement

Les forces et les industriels s'appuient sur des environnements numériques immersifs, des jumeaux numériques et des capacités de calcul intensif pour concevoir les systèmes, préparer les missions, entraîner les équipages et valider les scénarios opérationnels.

Logistique, soutien et maintien en condition opérationnelle (MCO)

Le suivi des ressources, la maintenance prédictive des équipements, la gestion du carburant, des munitions et des pièces détachées reposent sur des systèmes numériques continus reliant les unités déployées, les bases arrière et les acteurs industriels.

IA militaire et aide à la décision

Analyse prédictive, détection d'anomalies, ciblage, guerre électronique, protection des forces : les modèles d'IA, développés et entraînés en lien avec l'industrie de défense, nécessitent des infrastructures locales sécurisées capables de fonctionner sur site, en environnement contraint ou embarqué.

Ces usages imposent **une infrastructure numérique capable d'opérer du centre nerveux stratégique jusqu'au terrain tactique** et aux plateformes industrielles ou embarquées, avec des niveaux d'automatisation, de résilience et de sécurité largement supérieurs à ceux des architectures classiques.

La guerre moderne impose une nouvelle lecture de la capacité militaire.

Un service public de proximité sous haute responsabilité.

Les forces armées disposent aujourd'hui d'infrastructures numériques robustes, capables de soutenir les opérations, le commandement, le renseignement, la logistique et le maintien en condition opérationnelle. Ces infrastructures remplissent leur mission et ont accompagné avec succès la montée en puissance du numérique dans les armées.

Cependant, le rythme et la nature des conflits contemporains ont profondément évolué.L'accélération des menaces, la réduction des cycles décisionnels, la multiplication des capteurs et l'explosion des volumes de données exercent une pression croissante sur des architectures souvent rigides, cloisonnées et complexes à faire évoluer.

Un environnement opérationnel en rupture

Les forces doivent désormais opérer dans des environnements hybrides, contestés et instables, où la continuité numérique, sa capacité à fonctionner en tout autonomie locale et sa résilience ne sont plus des options mais des prérequis. Les infrastructures historiques peinent à absorber simultanément les besoins en IA, en traitement temps réel, en mobilité tactique et en sécurité renforcée face à des adversaires étatiques technologiquement avancés.

Dans ce contexte, faire évoluer l'existant constitue un levier essentiel pour consolider et prolonger l'avantage militaire.

Conserver l’avantage en amplifiant les capacités de l’infrastructure numérique.

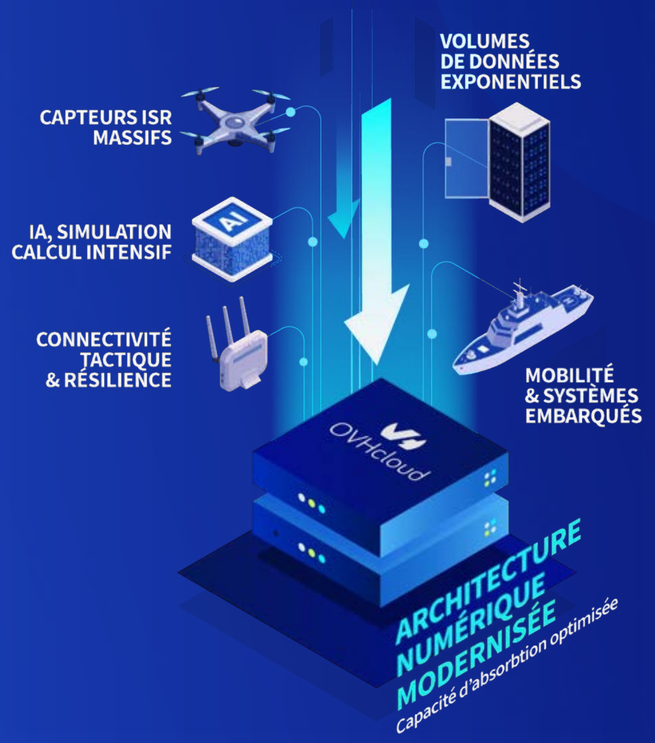
Aller au-delà du maintien en condition

Conserver une longueur d’avance ne consiste plus uniquement à moderniser ponctuellement les systèmes, mais à disposer d’une infrastructure capable d’évoluer en permanence au rythme des besoins opérationnels. L’enjeu est de transformer un socle numérique fonctionnel en un levier de supériorité durable, capable d’intégrer rapidement de nouvelles capacités sans fragiliser les opérations en cours.

Cela implique une infrastructure suffisamment flexible pour accueillir l’innovation — IA, automatisation, exploitation avancée de la donnée — tout en restant pleinement maîtrisée, souveraine et sécurisée.

Innover sans rupture, opérer sans dépendance

L’innovation militaire doit être continue, incrémentale et maîtrisée, directement au service de la manœuvre et de la décision.
Dans la guerre moderne, la capacité à survivre, à s’adapter et à innover plus vite que l’adversaire est devenue une condition déterminante de la supériorité militaire.
L’infrastructure numérique n’est plus un simple support : **elle constitue désormais une capacité militaire à part entière**, au cœur de la liberté d’action des forces.



Une transformation numérique impérative : l'obsolescence comme risque stratégique.

Les forces armées et l'industrie de défense font aujourd'hui face à des architectures numériques, conçues pour des contextes opérationnels et industriels qui ne correspondent plus aux exigences actuelles :

- → cloisonnées entre armées, programmes et acteurs industriels,
- → hétérogènes dans leurs technologies et leurs niveaux de maturité,
- → vieillissantes et difficiles à faire évoluer,
- → peu adaptées aux déploiements rapides ou aux environnements embarqués,
- → fréquemment non interopérables, y compris entre systèmes conçus pour opérer ensemble,
- → coûteuses à maintenir sur des cycles de vie qui s'étendent sur plusieurs décennies.

Ces architectures peinent à absorber :

- → l'augmentation massive des capteurs ISR intégrés aux plate formes et aux théâtres d'opérations,
- → les besoins croissants de calcul pour l'IA, la simulation et l'analyse avancée,
- → les exigences de connectivité tactique et de résilience en environnement contesté,
- → les volumes exponentiels de données stratégiques et industrielles,

L'obsolescence à venir de ces infrastructures, dû aux nouveaux usages, est devenue un **risque militaire et industriel majeur** : elle limite l'agilité opérationnelle, rallonge les cycles de décision, complique la coordination interarmées et inter-programmes, freine l'évolution des plateformes et expose les forces à des vulnérabilités critiques.

Dans ce contexte, la modernisation numérique n'est plus un simple projet informatique :**c'est une condition indispensable de supériorité opérationnelle, de cohérence industrielle et de souveraineté durable.**

Le cloud on-premise de Défense moderne : un cloud qui s'adapte à tous les théâtres d'opérations.

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 :

Déploiement rapide
Mise en place automatisée d'un environnement opérationnel complet en quelques minutes, aussi bien pour un poste de commandement, une base avancée, une plateforme embarquée ou un site industriel sensible.

Opérations sur site
Fonctionnement local et autonome pour les bases avancées, les navires, les détachements projetés, les postes de commandement tactiques, ainsi que pour les plateformes et ateliers industriels opérant en environnement contraint.

Air-gap intégral
Aucune dépendance réseau, aucune interconnexion obligatoire : capacité à opérer durablement en isolement total, que ce soit sur un théâtre d'opérations, à bord d'une plateforme stratégique ou dans un environnement industriel classifié.

Automatisation extrême
Réduction significative de la charge pour les unités SIC et les équipes industrielles grâce à des opérations standardisées, fiabilisées et largement automatisées, même en environnement dégradé.

Calcul tactique
Latence ultra-faible pour l'IA embarquée, les drones, les radars, les systèmes optroniques et les capteurs intégrés aux plateformes, avec des capacités de calcul déployées au plus près des systèmes d'armes.

Protection renforcée
Durcissement cyber de niveau militaire, intégrant des mécanismes de protection avancés pour les environnements opérationnels, industriels et embarqués.

Interopérabilité contrôlée
Capacité à dialoguer avec des clouds externes ou des systèmes partenaires lorsque cela est nécessaire, sans dépendance structurelle ni perte de souveraineté.

Ce type de cloud constitue désormais un multiplicateur de puissance opérationnelle et industrielle, au cœur de la supériorité militaire moderne.

OPCP : une plateforme cloud conçue pour la Défense, du stratégique à la tactique.

OPCP est une plateforme cloud-native on-premise, capable d'opérer dans les environnements suivants :

- → datacenters Défense,
- → industries de Défense,
- → sites informatique classifiés,
- → PC de théâtre opérationnel,
- → navires,
- → bases projetées,
- → zones hostiles,
- → environnements déconnectés.

Elle offre :

- → déploiement automatisé,
- → prêt pour le durcissement militaire,
- → Gouvernance informatique interarmées,
- → résilience numérique,
- → autonomie totale en mode isolé,
- → Orchestration des services.

OPCP apporte à la Défense une architecture unifiée, conçue pour les armées ainsi que l'industrie, et capable d'accompagner la montée en puissance IA, cyber, C4ISR moderne.

LANDING ZONE MANAGER

La gouvernance :

- → isolation stricte par unité, mission, projet,
- → politiques de classification,
- → contrôle d'accès avancé,
- → supervision nationale ou locale.

CLOUD STORE

Le catalogue militaire :

- → applications C4ISR,
- → moteurs IA tactiques,
- → environnements analytiques,
- → services déployables rapidement, y compris en air-gap.

OPCP CORE

La fondation sécurisée :

- → orchestration compute / réseau / sécurité,
- → patching automatisé,
- → résilience multi-niveaux,
- → autonomie en site isolé,
- → observabilité complète pour centres de commandement.

Le cloud on-premise comme Multiplicateur de Puissance Militaire.

Les Use Cases présentés illustrent comment une infrastructure cloud de nouvelle génération, telle qu'OPCP, répond aux exigences concrètes de l'écosystème Défense, depuis le niveau stratégique jusqu'au niveau tactique et industriel.

Ils montrent comment le cloud devient un véritable multiplicateur de puissance militaire, permettant de renforcer **la résilience, d'accélérer le cycle décisionnel et d'augmenter durablement la capacité d'action sur l'ensemble du spectre des opérations militaires et industrielles.**

OPCP

USE CASE | **01**

Poste de Commandement numérique projetable & résilient.

Le tempo des opérations modernes exige des postes de commandement (PC) capables d'être :

- → **déployés rapidement,**
- → **opérationnels en quelques minutes,**
- → **résilients aux attaques,**
- → **autonomes en réseau,**
- → **interopérables avec les unités alliées.**

Dans les environnements contestés, la chaîne C4ISR doit survivre, même en cas de brouillage, de coupure satellite ou de pression cyber.

OPCP apporte :

- → **Un déploiement entièrement automatisé** des services, renseignement, planification et suivi des opérations.
- → Une **architecture capable de fonctionner en mode isolé**, sans liaison avec le commandement arrière.
- → Une **résilience multi-niveaux** : basculement local, reprise instantanée et primitives de sécurité permettant l'implémentation d'un durcissement cyber intégré.
- → La **capacité d'exécuter localement** les applications critiques.
- → Des **performances stables** même en conditions extrêmes (climat, mobilité, opérations de haute intensité).

Le PC devient un véritable centre névralgique numérique, mobile, autonome et robuste, capable de conserver l'initiative même lorsque l'espace informationnel est contesté.

OPCP

USE CASE | **02**

Exploitation Souveraine du Renseignement ISR & IA Militaire.

Le volume, la diversité et la vitesse du renseignement moderne imposent un traitement local sécurisé : IMINT, SIGINT, HUMINT, OSINT, ROEM, radars, satellites, drones tactiques, guerre électronique…

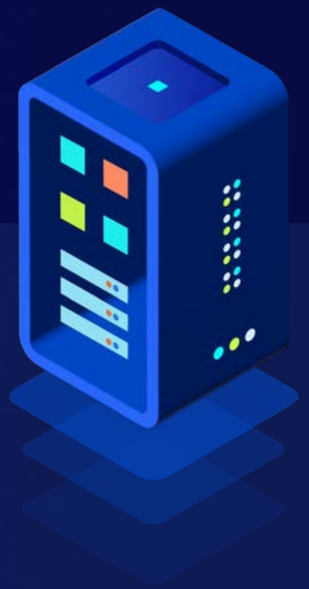
Les armées doivent pouvoir :

- **ingérer, fusionner et analyser** des flux hétérogènes,
- entraîner et exploiter des **modèles IA militaires** sur site,
- assurer un traitement **immédiat**, même sans réseau global,
- protéger des **données classifiées** niveau Secret ou Très Secret.

OPCP permet :

- Un **traitement souverain des données** sensibles, sans transfert vers un fournisseur externe.
- L'**inférence de modèles IA** directement dans le théâtre d'opération.
- La prise en charge de **pipelines ISR automatisés** : ingestion → corrélation → analyse → décision.
- Un fonctionnement en **air-gap complet**, éliminant tout risque de fuite.
- Une **diffusion contrôlée** vers les niveaux stratégique, opératif et tactique.

La boucle renseignement-décision-action est accélérée, sécurisée, et rendue indépendante de toute contrainte de souveraineté ou de communication.



OPCP

USE CASE | 03

Cloud Tactique pour Unités Projetées

Dans ces environnements isolés, parfois déployés plusieurs mois sans connexion fiable, les systèmes numériques embarqués doivent continuer à opérer, à traiter des données sensibles et à soutenir la conduite des opérations, même en cas de dégradation ou de perte totale des liaisons externes.

Pour cela, les unités projetées doivent disposer d'un cloud : → compact → durci → autonome, → capable d'opérer avec **une empreinte logistique minimale.**

Les opérations exigent un calcul local pour :
- → IA embarquée (détection, classification, trajectographie),
- → traitement des flux capteurs,
- → gestion tactique du combat,
- → communications et échanges distribuée.

OPCP apporte :
- → Un **cloud tactique robuste** capable de fonctionner dans un PC mobile, un bâtiment de la flotte ou un détachement avancé.
- → Un **calcul local avec très faible latence** grâce à une proximité tactique avec tous les systèmes d'armes.
- → Une **synchronisation différée** en cas de reconnexion, sans perte de données.
- → Une **automatisation** qui réduit le besoin en personnel spécialiste.
- → Une **continuité totale des services** même en mobilité ou déconnexion.

Les forces gagnent en autonomie, en vitesse décisionnelle et en supériorité informationnelle le tout sans dépendre d'un cloud central.

OPCP

USE CASE | **04**

Résilience Nationale en Situation de Crise ou d'Attaque Cyber.

Un cloud complétement isolé et autonome.

Les cyberattaques étatiques visant les infrastructures nationales peuvent paralyser :

- les communications,
- la logistique,
- les systèmes financiers,
- les centres de commandement,
- les systèmes d'alerte,
- les bases militaires.

Les armées doivent conserver une capacité d'action **même en cas d'effondrement temporaire du numérique national.**

OPCP permet :

- Le **maintien opérationnel des applications critiques** (santé militaire, carburant, munitions, RH, C4ISR).
- Une **capacité de reconstruction rapide** après compromission du système central.
- Une **résilience par zones** : chaque site peut fonctionner comme un îlot souverain.
- La **possibilité d'un durcissement cybersécurité** conforme aux standards militaires et agences nationales de sécurité.
- Une **isolation instantanée** d'un site compromis sans rupture des autres zones.

L'Etat reste ainsi capable de se défendre, de commander ses forces et de coordonner ses ressources, même lors d'une attaque cyber massive.

OPCP

USE CASE | **05**

Interopérabilité & Mutualisation Interarmées / Interalliés.

Les opérations modernes sont multi-domaines et s'appuient sur :
- → l'armée de Terre,
- → l'armée de l'Air et de l'Espace,
- → la Marine,
- → les unités de défense Cyber,
- → le Renseignement,
- → les différentes coalitions (OTAN, partenariats bilatéraux, missions ONU).

Les systèmes d'information doivent donc être :
- → Harmonisés dans leur fonctionnement,
- → Compatibles technologiquement,
- → segmentés selon les niveaux de classification,
- → gouvernés de manière cohérente.

OPCP apporte :
- → un **socle unifié** pour toutes les armées et agences du ministère de la Défense.
- → Une **isolation stricte** par périmètre (unités, mission, projets).
- → Des **politiques de sécurité adaptées** aux niveaux de classification (Secret → Très Secret).
- → Une **standardisation des déploiements**, réduisant les coûts et les risques.
- → Une **capacité de collaboration sécurisée** avec les forces alliées.

Par conséquent, la Défense gagne en cohérence, en efficacité opérationnelle et en capacité de mener des opérations conjointes ou combinées.

OPCP

USE CASE | **06**

Cloud Industriel Souverain pour Conception, MCO et Évolution des Systèmes d'Armes.

L'industrie de défense doit gérer des systèmes d'armes et plateformes critiques conçus pour opérer sur plusieurs décennies, ce qui impose des infrastructures numériques capables de :

- supporter des cycles de vie longs et complexes,
- traiter des données sensibles et classifiées,
- accompagner l'évolution continue des capacités,
- garantir la continuité entre conception, production et exploitation,
- assurer une souveraineté totale sur les données et les modèles.

Dans ce contexte, les environnements numériques industriels doivent rester opérationnels, sécurisés et cohérents, tout en permettant des échanges maîtrisés avec les forces armées, sans exposition ni dépendance externe.

OPCP apporte :

- Un **cloud industriel on-premise souverain**, utilisé pour la conception, la simulation, les tests et le maintien en condition opérationnelle (MCO).
- La **prise en charge de jumeaux numériques**, de simulations massives et de calculs IA sur données sensibles.
- Une **continuité numérique** entre industriels, autorités étatiques et forces armées, avec des périmètres strictement cloisonnés.
- Une **capacité à déployer des environnements de travail sécurisés** sur sites industriels, bases de soutien ou centres de maintenance.
- Une **modernisation progressive des systèmes numériques industriels** sans rupture des programmes existants.

L'industrie de défense dispose ainsi d'un socle numérique unifié, souverain et pérenne, garantissant la disponibilité, l'évolution et la performance des capacités militaires dans la durée.

Une complémentarité qui a du sens

D’un côté, une solution technique éprouvée.
De l’autre, une connaissance fine du terrain.
Il est clair qu’il y a des choses à faire ensemble.

Des cas à inventer, adapter, tester

Les cas d’usage ne manquent pas : edge, usines, sites critiques, infrastructures déconnectées…
Et si on en identifiait un ou deux pour avancer concrètement ?

Un atelier, un échange, un POC ?

Pas besoin de tout figer d’emblée.
Juste un moment pour creuser ensemble, voir ce qui a du sens, et construire, pas à pas.

ovhcloud.com
opcp@ovhcloud.com