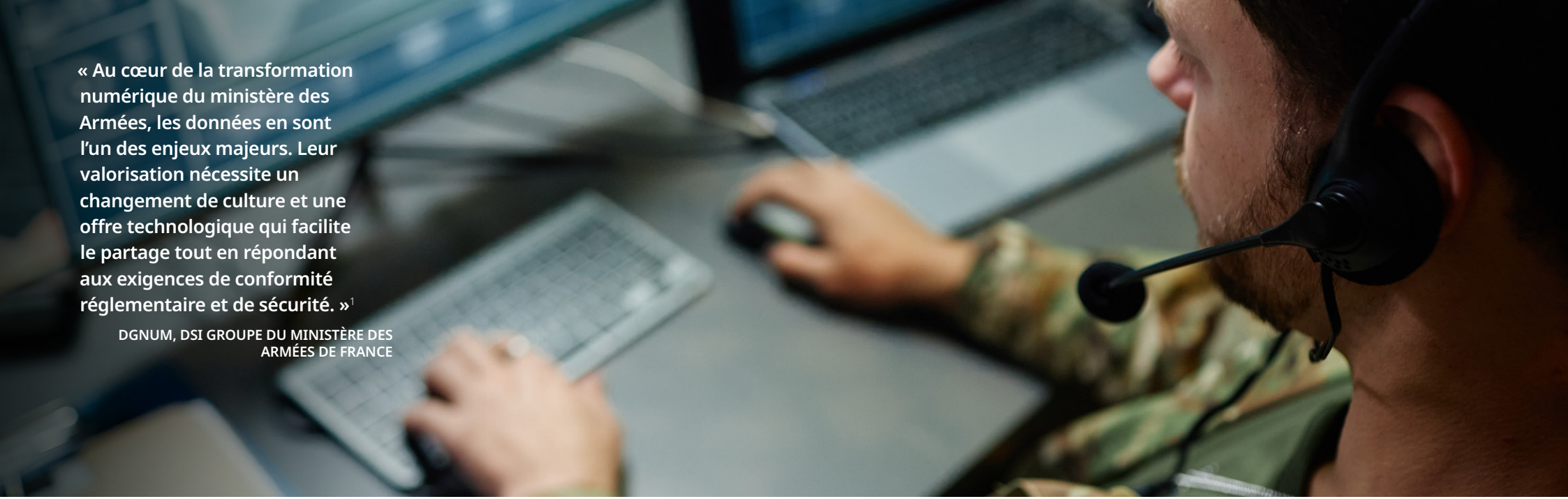
Le rôle des technologies avancées dans une base intelligente

Livre blanc

Alcatel·Lucent
Enterprise

Sommaire



« Au cœur de la transformation numérique du ministère des Armées, les données en sont l'un des enjeux majeurs. Leur valorisation nécessite un changement de culture et une offre technologique qui facilite le partage tout en répondant aux exigences de conformité réglementaire et de sécurité. »[1]

DGNUM, DSI GROUPE DU MINISTÈRE DES ARMÉES DE FRANCE

Introduction

En matière de technologie de pointe, le secteur de la défense est réputé pour sa sophistication. Qu'elles soient développées en interne ou dans le commerce, les organisations de défense du monde entier adoptent et adaptent agressivement les technologies afin de les appliquer à des scénarios de combat et de guerre. Le moteur de leur stratégie est de plus en plus axé sur l'acquisition, la distribution ou la gestion des données.

Cela est dû non seulement au volume important de données, qui connaît une croissance annuelle à deux chiffres, mais aussi à la nature du paysage des menaces, désormais beaucoup plus complexe en raison de la nécessité de surveiller et de traiter en permanence le problème grandissant de la cybercriminalité et de la désinformation.

C'est là qu'une stratégie de transformation numérique est cruciale. En tirant parti des technologies de l'information et de la communication (TIC) pour tout connecter et en tout lieu, le secteur peut davantage exploiter pleinement les données disponibles et les transférer de manière plus efficace et plus sûre au sein de leurs organisations.

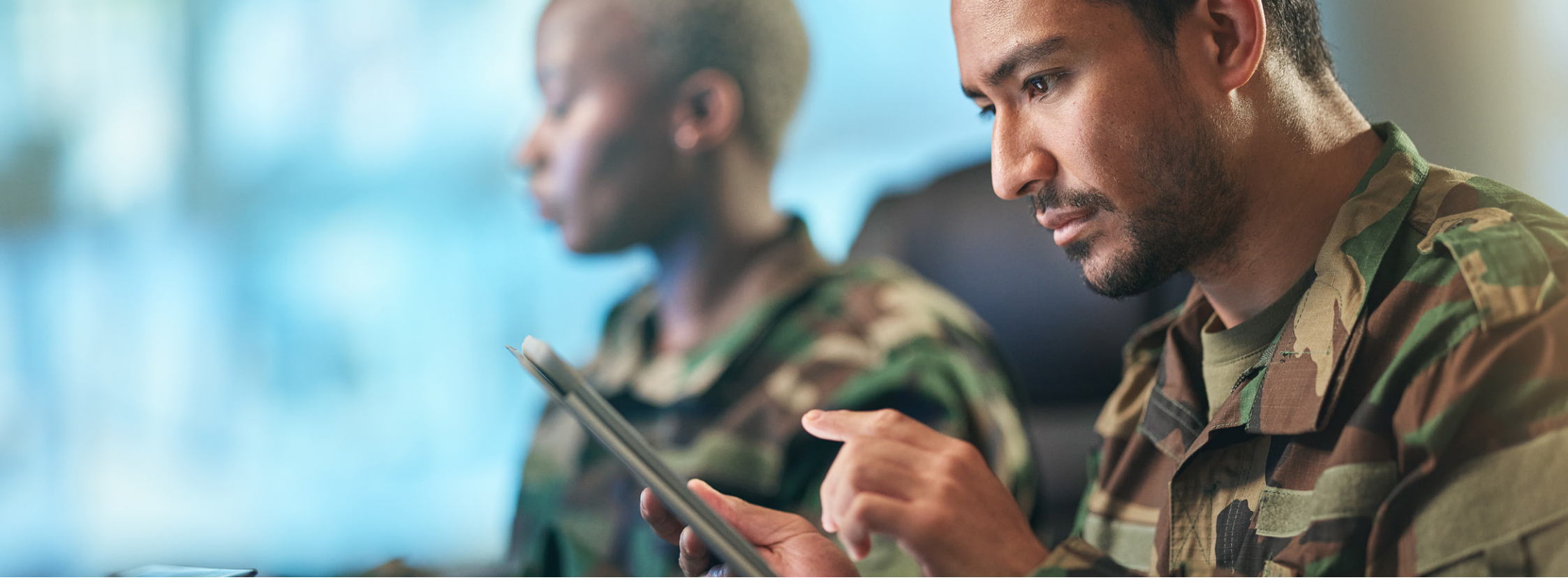
Si les structures existantes - telles que l'administration, les lieux de travail et les bureaux - ont pu ralentir une transformation dans le passé, les TIC ont progressé au point que bon nombre de ces préoccupations ne constituent plus des obstacles au progrès.

Dotées de la bonne stratégie de transformation numérique et des technologies TIC appropriées, les organisations de défense peuvent désormais tout connecter, partout. Cela leur permettra de créer des bases intelligentes, à partir desquelles elles pourront atteindre plus efficacement les objectifs opérationnels en temps de paix et de conflit, faire face plus efficacement aux cybermenaces et attirer et retenir plus facilement les meilleurs talents.

L'accès opportun à des données de qualité peut offrir des avantages significatifs. Cela se traduit par une optimisation des processus au siège et sur les bases militaires, une prise de décision plus éclairée sur le terrain, ainsi qu'une meilleure intégration du personnel et des équipements connectés, qu'ils soient sur terre, dans les airs, en mer, dans l'espace ou dans le cyberespace.

Dans ce document, nous examinerons les obstacles auxquels les organisations de défense sont confrontées lorsqu'elles entreprennent une transformation numérique, ainsi que les facteurs qui les incitent à franchir le pas. Nous aborderons également les principaux enseignements tirés des organisations des secteurs public et privé qui se sont déjà transformées et la manière dont ces enseignements peuvent être transposés dans le secteur de la défense.

1 - "Enjeux de la transformation numérique : la maîtrise et la valorisation des données" DGNUM, septembre 2022.



Les obstacles au changement

Structure interne

L'un des plus grands obstacles à la transformation numérique dans le secteur de la défense est la nature même des organisations de défense. Les cloisonnements commerciaux et technologiques ont créé un environnement opérationnel unique avec des systèmes de communication obsolètes - tels que la téléphonie PBX - qui ne peuvent pas prendre en charge les fonctions de communication et de collaboration modernes.

Pour la plupart, les systèmes existants fonctionnent dans un environnement indépendant non connecté à Internet ou à une infrastructure Cloud.

Ainsi, alors qu'une grande partie du monde a commencé à migrer vers la technologie IP il y a 10 ou 20 ans déjà, le secteur de la défense a résisté pour diverses raisons :

- **La sécurité :** le respect de la réglementation, les exigences en matière de protection de la vie privée et la nécessité de protéger les données sensibles ont rendu difficile l'adoption d'une technologie susceptible d'être violée
- **Culture et gouvernance :** une structure de gestion descendante exigeant l'approbation de l'échelon supérieur pour les initiatives de changement majeures a empêché l'armée de profiter de l'afflux de milléniaux et de natifs du numérique dans les secteurs privé et public, qui ont créé une pression ascendante en faveur de l'adoption des technologies numériques
- **Le budget :** avec des ressources limitées, le maintien de l'état de préparation de l'équipement et du personnel a été la priorité
- **La concurrence :** contrairement aux industries commerciales, le secteur de la défense ne possède pas de concurrents directs dans l'économie et a été principalement axé sur la garantie de la prouesse technologique des équipements du champ de bataille et des systèmes de guerre connectés

Les moteurs du changement

Géopolitique et technologie

Alors que ces obstacles entravent la transformation numérique, le monde a connu des changements spectaculaires.

La pandémie et l'instabilité géopolitique ont montré à quelle vitesse les chaînes d'approvisionnement mondiales pouvaient être perturbées, avec des répercussions importantes sur les économies locales.

De plus, le rythme auquel la technologie évolue a eu un impact sur les exigences en matière de gestion des données.

Les progrès réalisés en matière d'apprentissage automatique, d'intelligence artificielle, de capteurs avancés et de systèmes autonomes sont à la base d'une génération d'armes connectées et plus sophistiquées. Ces technologies jouent toutes un rôle majeur dans les efforts de défense sur le champ de bataille et en dehors. Elles amorcent une évolution vers un processus de gestion plus centré sur les données à l'intérieur du pays et pendant les conflits.

Pour optimiser les processus et maintenir un état de préparation, chaque organisation de défense doit rechercher des moyens efficaces et efficients pour collecter, stocker et distribuer toutes les données supplémentaires générées par ces nouveaux systèmes.

Coopération interdomaines

Les changements plus spécifiques apportés au cadre dans lequel les organisations de défense doivent désormais opérer ne font qu'aggraver la situation.

Les délimitations traditionnelles des opérations aériennes, terrestres et maritimes ont cédé la place à une vision globale plus complexe. Pour être efficaces, ces silos indépendants doivent désormais faire partie d'un cadre stratégique hautement connecté, axé sur des opérations multidomaines et fondé sur la circulation transparente des données au sein de tous les domaines et entre eux.

L'OTAN, par exemple, a ajouté l'espace et la cyberspace à ses opérations maritimes, terrestres et aériennes traditionnelles, reconnaissant ainsi la menace des données et la nécessité de mieux orchestrer ces domaines.

Les accords de coopération en matière de défense mentionnés par Brandon J. Kinne dans son article Defense Cooperation Agreements and the Emergence of a Global Security Network viennent encore compliquer la situation : « ...établir des cadres institutionnels à long terme pour les relations bilatérales de routine en matière de défense, y compris la coordination des politiques de défense, les exercices militaires conjoints, les groupes de travail et les comités, les échanges en matière de formation et d'éducation, la recherche et le développement liés à la défense et les achats ».[2]

Ces accords reposent sur de nouveaux modèles opérationnels fondés sur le partage d'informations, des opérations dynamiques interconnectées, une prise de décision agile et rapide, une coordination en temps réel et la nécessité d'une sécurité et d'une résilience de l'information.

2 - "Defense Cooperation Agreements and the Emergence of a Global Security Network," Cambridge University Press, 2018.

« La structure de l'OTAN comprend cinq domaines d'opérations : maritime, terrestre, aérien, spatial et cyberspace. Historiquement, les opérations dans ces domaines n'ont jamais existé (espace et cyberspace) ou ont fonctionné comme des entités largement indépendantes au sein des armées nationales. Aujourd'hui, les armées de nombreux pays alliés fonctionnent encore de cette manière. Cependant, compte tenu de la vitesse de l'information, des flux de données et des capacités adverses, la nécessité d'orchestrer les activités militaires dans tous les domaines en tant que force unique est cruciale pour les initiatives de défense et de dissuasion à long terme au sein de l'OTAN. »[3]

3 - "Multi-Domain Operations in NATO – Explained," NATO, octobre 2023.

Des processus de données efficaces et sécurisés

En fin de compte, pour permettre des opérations multi-domaines et soutenir les accords de coopération en matière de défense, l'ensemble des organisations de défense ont besoin de systèmes capables de déplacer des données de manière plus efficace et plus sûre. Par conséquent, elles adoptent rapidement les normes IP et les technologies de l'Internet des objets militaires (IoMT) et les systèmes afin de répondre à la nécessité de collecter et de traiter un nombre croissant de données contextuelles provenant des navires, des véhicules et des engins sans pilote, ainsi que sous forme d'objets portables pour les soldats augmentés.

Mais si les technologies IoMT peuvent collecter des données, il est toujours difficile de les fournir, distribuer et traiter efficacement. De nombreuses organisations de défense s'interrogent ainsi aujourd'hui sur la meilleure façon d'optimiser les processus en faisant converger les systèmes indépendants de technologie opérationnelle (OT) et de technologie de l'information (IT) en un seul cadre opérationnel consolidé.

En outre, l'évolution et la sophistication de la technologie ont permis aux États de mener une cyberguerre plus efficace. Par conséquent, le champ d'application des efforts de protection de la défense doit désormais inclure des capacités de dissuasion numérique contre les cyberattaques visant les infrastructures critiques, ainsi que contre les campagnes de désinformation.

Il est évident qu'être dotés de systèmes TIC dépassés et obsolètes ne facilite pas la tâche. Plus important encore, ces systèmes dépassés et obsolètes ne peuvent pas prendre en charge les opérations multidomaines qui incluent le domaine cyberspace. Ils ne peuvent pas non plus soutenir les accords de coopération en matière de défense avec les pays partenaires qui doivent partager des informations et être assurés que celles-ci seront protégées et sécurisées.

Attirer et retenir les employés

Le secteur de la défense est confronté aux mêmes défis que les entreprises commerciales : comment attirer et retenir les meilleurs talents. Les organisations de défense doivent disposer d'outils TIC pour former le personnel dans tous les domaines, créer un environnement de travail efficace et gratifiant et permettre l'équilibre entre vie professionnelle et vie privée désormais attendu par les employés.

« ...une entreprise véritablement connectée permettra l'intégration, au niveau national et international, des cinq domaines : maritime, terrestre, aérien, cyberspace et spatial. La défense pourra ainsi exploiter pleinement la puissance de ses données, en connectant les capteurs, les décideurs et les effecteurs à grande échelle et à grande vitesse. »[4]

MINISTÈRE DE LA DÉFENSE DU ROYAUME-UNI

4 - "Data Strategy for Defence: Delivering the Defence Data Framework and Exploiting the Power of Data," UK Ministry of Defence, septembre 2021.

Les enseignements tirés des secteurs public et privé

Bien que ces facteurs externes constituent tous des moteurs de changement, de nombreuses organisations de défense peinent encore à adopter des stratégies de transformation numérique, même si cette dernière s'est avérée être un moyen efficace pour les entreprises publiques et privées de créer des gains d'efficacité et d'améliorer les opérations. De nombreux personnels de la défense n'étant pas des combattants, les approches de la transformation et les enseignements tirés s'appliquent également aux bâtiments administratifs de la défense et aux bases militaires.

Les technologies de l'information et de la communication ont également évolué au point que la plupart des préoccupations technologiques du passé n'ont plus lieu d'exister. Des solutions numériques rentables et faciles à déployer, basées sur des protocoles standard, sont disponibles pour soutenir les lieux de travail de la défense numérique grâce à des communications et à une collaboration efficaces. Et nombre d'entre eux offrent le niveau élevé de défense en matière de cybersécurité dont les organisations ont besoin.

La transformation numérique stratégique équipera les organisations de défense pour mieux faire face à la nouvelle réalité dans laquelle elles opèrent. Une transformation efficace créera un environnement numérique sécurisé dans lequel toutes les données disponibles pourront être déplacées plus rapidement et de manière plus sûre afin de soutenir et d'habiliter le personnel dans tous les domaines.

Pour créer cet environnement, les organisations de défense peuvent appliquer des approches éprouvées de la transformation numérique issues des secteurs privé et public.

Dans la section suivante, nous examinerons les enseignements tirés du déploiement de stratégies de transformation numérique dans les secteurs public et privé ainsi que la manière dont ces enseignements peuvent s'appliquer aux organisations de défense.

Bâtiments intelligents et infrastructures hyperconnectées

Les bâtiments intelligents font désormais partie des centres urbains du monde entier et peuvent facilement

être créés dans les centres d'administration de la défense et les bases militaires. Ces bâtiments exploitent les technologies IoT pour tout surveiller et gérer intelligemment, de l'éclairage et de la chaleur aux systèmes de surveillance des principaux points d'accès et de sortie.

L'évolution constante des technologies IoT a rendu possible la création d'infrastructures hyperconnectées. Ces structures connectées numériquement combinent l'automatisation opérationnelle et la gestion contextuelle de l'espace afin d'adapter intelligemment le fonctionnement du bâtiment aux schémas de circulation dans les zones clés et aux besoins de confort et de sécurité de ses occupants et de son environnement. Il en résulte des espaces intelligents qui rendent les lieux de travail plus sûrs, plus sains et plus conviviaux, en améliorant l'expérience des employés, et augmentant ainsi la productivité.[5]

Concepts de villes intelligentes

Les bases militaires étant semblables à des villes autonomes, les bâtiments intelligents et les infrastructures hyperconnectées sont les composantes essentielles pour créer des bases intelligentes basées sur des concepts de ville intelligente éprouvés.

Les bases intelligentes exploitent les données disponibles sur une base et créent « une infrastructure intelligente sécurisée, des bâtiments économes en énergie, des transports efficaces, des opérations rentables et une meilleure qualité de vie pour les habitants ».[6]

L'infrastructure réseau qui permet la mise en place d'une base intelligente peut également être utilisée pour créer un dispositif de sécurité plus efficace qui protège non seulement les données sur la base, mais aussi la sécurité physique du personnel et des installations. Cela peut être réalisé avec des systèmes de sécurité avancés, tels que des systèmes de surveillance du périmètre et de détection des intrusions créés avec des solutions IoT et IA connectées à des centres de sécurité.

La création de bases intelligentes va au-delà de l'installation de capteurs et de systèmes les plus récents. Il s'agit d'intégrer toutes les technologies et tous les processus existants et nouveaux dans un cadre cohérent de réseau TIC reposant sur les technologies les plus avancées et déployé par le biais d'une transformation numérique stratégique.

Et cette transformation peut également s'appliquer à d'autres domaines, par exemple :

- les opérations sur le terrain, où les technologies TIC sont utilisées comme l'épine dorsale des réseaux d'information sur les navires et les véhicules militaires, et comme le lien pour un combattant connecté qui tire parti de capteurs et d'équipements portables sophistiqués
- les centres de commandement et de contrôle, où les technologies de l'information et de la communication facilitent le soutien aux opérations de défense civile ou la gestion des crises avec d'autres agences gouvernementales lors de catastrophes naturelles

Le pouvoir des TIC avancées

Grâce aux technologies TIC les plus avancées, les organisations de défense seront mieux équipées pour partager des informations, coordonner des stratégies et gérer des opérations conjointes dans le monde entier.

La clé d'une transformation numérique efficace est un cadre stratégique de communication et de réseau spécialement conçu et optimisé pour la base intelligente.

Ce réseau doit être sécurisé, robuste et conçu pour prendre en charge toutes les connexions à tout moment afin de déplacer plus efficacement d'énormes volumes de données. Et il doit être construit avec des solutions TIC qui soutiennent l'intégration et l'interconnexion des opérations administratives, des bases militaires, du personnel déployé et des actifs sur terre, dans l'air, en mer et dans l'espace, et la maîtrise des menaces croissantes et pernicieuses générées dans le cyberespace.

5 - "Smart Buildings Get Hyperaware," John Hatcher, Smart Buildings Magazine, août 2020.
6 - "Building the Smart Base of the Future," Laura A. Nolan, National Strategic Research Institute, mars 2020.

ALE : un partenaire pour la transformation numérique

Alcatel-Lucent Enterprise comprend les défis auxquels les organisations de défense sont confrontées lorsqu'elles planifient et développent des stratégies de transformation numérique qui s'appuient sur les technologies TIC pour répondre aux exigences de l'armée d'aujourd'hui.

Chez ALE, nous soutenons la transformation numérique à l'aide de solutions résilientes et sécurisées pour la défense connectée, notamment :

- Des solutions LAN et WLAN basées sur l'IoT, y compris des commutateurs renforcés qui couvrent tous les besoins en matière de réseau de ville connectée et fournissent l'intégration de l'IoT sécurisée et automatisée pour un certain nombre d'exigences de défense
- Des solutions de communication, de collaboration et CPaaS pouvant être fournies sur site (Cloud privé), dans le Cloud (Cloud public) ou en mode hybride
- Des solutions d'automatisation des flux de travail et des processus qui surveillent, détectent et traitent de manière proactive les problèmes avant qu'ils ne se posent, permettant ainsi d'accroître l'efficacité opérationnelle et de réduire les coûts
- La sécurité selon une approche Privacy by design dans un cadre Zero Trust, et avec des certifications pertinentes en matière de confidentialité des données

Les solutions de communication et de mise en réseau d'ALE peuvent être optimisées pour créer des architectures redondantes qui relient tout et tout le monde dans un cadre cohérent, entièrement intégré et hautement disponible.

Par ailleurs, nos solutions sont conçues dans un souci de sécurité maximale. Nous respectons strictement les pratiques et les normes de sécurité en vigueur et intégrons dans nos produits une série de technologies connexes, sans frais supplémentaires. La sécurité repose sur une approche par couches qui comprend l'intégrité du réseau, la sécurité des appareils et les politiques d'accès basées sur les profils des utilisateurs et la visibilité des applications. Les logiciels de réseau sont vérifiés par la validation du code sous-jacent par une tierce partie. Les systèmes IoT et les utilisateurs sont automatiquement et en toute sécurité intégrés et placés dans des conteneurs, qui sont structurés de manière à empêcher les cyberattaques potentielles à partir d'un appareil compromis. L'ensemble des données et des communications sont chiffrées à l'aide de mécanismes de chiffrement puissants afin d'éviter les écoutes clandestines et les attaques de type « man-in-the-middle ».

Afin de vous offrir une plus grande tranquillité d'esprit, nos solutions sont aussi conformes aux certificats de sécurité les plus stricts délivrés par des organisations indépendantes et des institutions gouvernementales.

En outre, notre cadre RRS (Risk, Resilience and Security) traite de la cybersécurité et de la sécurité physique pour les secteurs du gouvernement et de la défense.

Nous comprenons également l'importance de la souveraineté des données. Nos applications basées sur le Cloud offrent des options d'hébergement flexibles - dans des centres de données avancés et hautement sécurisés construits pour fournir des performances rapides et fiables, ou sur site avec notre solution de Cloud privé, Rainbow Edge. Les données stockées dans le Cloud appartiennent à nos clients, et nous ne fournissons ni ne vendons de données à aucune autre entreprise ou aucun autre pays.

En savoir plus

Pour en savoir plus sur les solutions Alcatel-Lucent Enterprise pour l'industrie de la défense, visitez notre site web ou contactez-nous pour découvrir comment nous pouvons vous aider à développer une stratégie de transformation numérique personnalisée pour votre organisation de défense.

Alcatel·Lucent
Enterprise