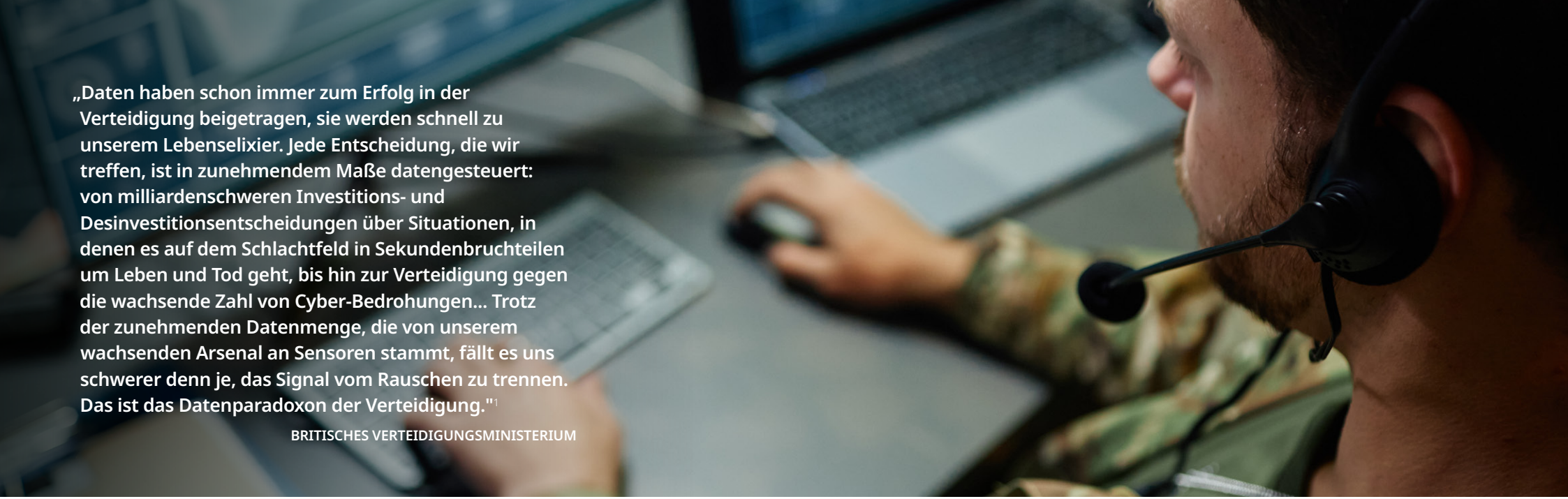
Die Bedeutung von Spitzentechnologie auf einem intelligenten Stützpunkt

Whitepaper

Alcatel·Lucent
Enterprise

Inhalt



„Daten haben schon immer zum Erfolg in der Verteidigung beigetragen, sie werden schnell zu unserem Lebenselixier. Jede Entscheidung, die wir treffen, ist in zunehmendem Maße datengesteuert: von milliardenschweren Investitions- und Desinvestitionsentscheidungen über Situationen, in denen es auf dem Schlachtfeld in Sekundenbruchteilen um Leben und Tod geht, bis hin zur Verteidigung gegen die wachsende Zahl von Cyber-Bedrohungen... Trotz der zunehmenden Datenmenge, die von unserem wachsenden Arsenal an Sensoren stammt, fällt es uns schwerer denn je, das Signal vom Rauschen zu trennen. Das ist das Datenparadoxon der Verteidigung."[1]

BRITISCHES VERTEIDIGUNGSMINISTERIUM

Einführung

Wenn es um Spitzentechnologie geht, ist der Verteidigungssektor für seine Raffinesse bekannt. Unabhängig davon, ob es sich um eine Eigenentwicklung oder um eine kommerzielle Entwicklung handelt, setzen Verteidigungsorganisationen auf der ganzen Welt auf die Übernahme und Anpassung von Technologien für den Einsatz in Kampf- und Kriegsführungsszenarien. Und der Erwerb, die Verteilung oder die Verwaltung von Daten wird immer mehr zur treibenden Kraft ihrer Strategie.

Das liegt nicht nur an der schieren Datenmenge, die jährlich zweistellig wächst, sondern auch an der Art der Bedrohungslandschaft, die durch die Notwendigkeit, das wachsende Problem der Cyberkriminalität und der Desinformation ständig zu überwachen und zu bekämpfen, noch viel komplizierter geworden ist.

Hier ist eine Strategie für die digitale Transformation von entscheidender Bedeutung. Durch den Einsatz von Informations- und Kommunikationstechnologien (IKT), um alles und überall zu vernetzen, kann der Sektor die verfügbaren Daten in vollem Umfang nutzen und sie effizienter und sicherer innerhalb ihrer Organisationen bewegen.

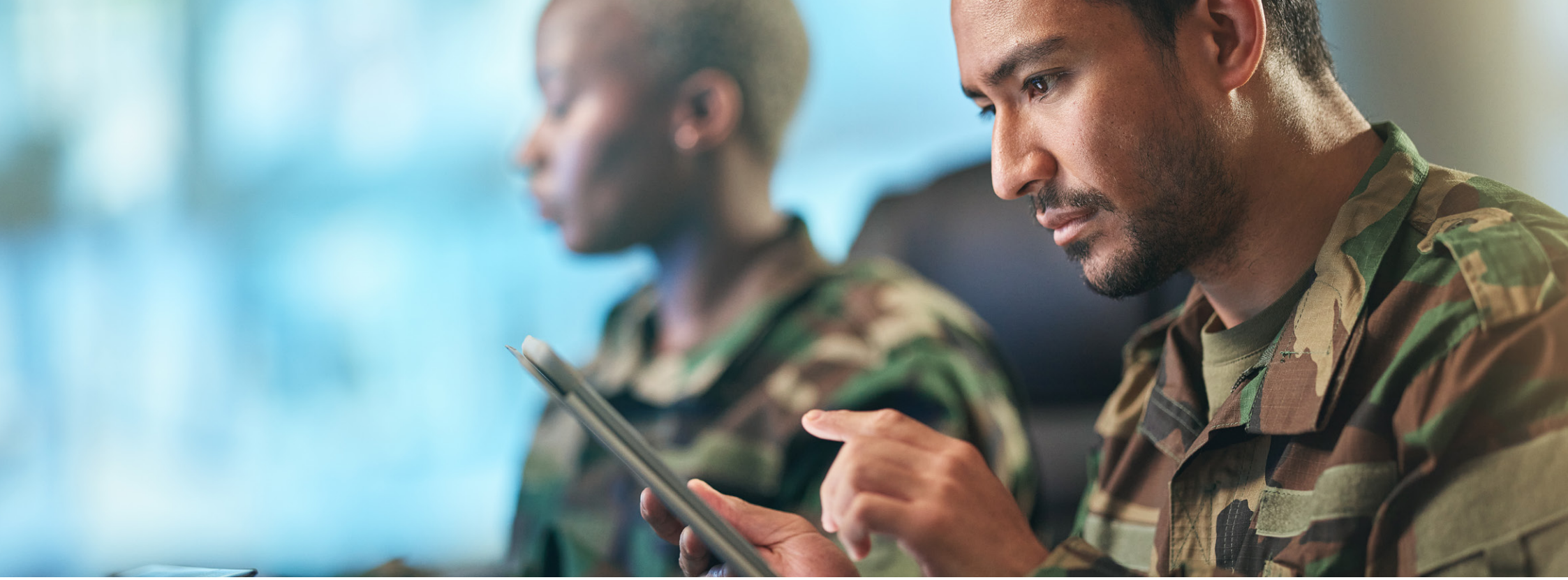
Während alte Strukturen - wie Verwaltung, Arbeitsplätze und Büros - in der Vergangenheit einen Wandel verlangsamt haben mögen, ist IKT inzwischen so weit fortgeschritten, dass viele dieser Bedenken nicht länger ein Hindernis für den Fortschritt darstellen.

Mit der richtigen Strategie für die digitale Transformation und den richtigen IKT-Technologien können Verteidigungsorganisationen jetzt alles und überall vernetzen. Auf diese Weise können sie einen intelligenten Stützpunkt schaffen, von dem aus sie die operativen Ziele in Friedens- und Konfliktzeiten effizienter erreichen, Cyberbedrohungen wirksamer bekämpfen und leichter Spitzenkräfte anwerben und halten können.

Die richtigen Daten zur richtigen Zeit können enorme Vorteile bringen: Optimierung von Prozessen im Hauptquartier und auf Militärstützpunkten, Unterstützung einer fundierteren Entscheidungsfindung im Feld und Erweiterung von vernetztem Personal und Ausrüstung in allen Zonen - zu Land, in der Luft, zur See, im Weltraum und im Cyberspace.

In diesem Whitepaper erörtern wir die Hindernisse, denen sich Verteidigungsunternehmen bei der digitalen Transformation gegenübersehen, sowie die treibenden Kräfte, die diese Transformation vorantreiben. Außerdem werden wir uns mit den wichtigsten Erkenntnissen von Organisationen des öffentlichen und privaten Sektors befassen, die bereits einen Wandel vollzogen haben, und mit der Frage, wie diese Erkenntnisse auf den Verteidigungssektor übertragen werden können.

1 - "Data Strategy for Defence: Delivering the Defence Data Framework and Exploiting the Power of Data", britisches Verteidigungsministerium, September 2021.



Hindernisse auf dem Weg zum Wandel

Interne Struktur

Eines der größten Hindernisse für die digitale Transformation im Verteidigungssektor liegt in der Natur der Verteidigungsorganisationen selbst. Geschäfts- und Technologiesilos haben eine einzigartige Betriebsumgebung mit veralteten Kommunikationssystemen - wie z.B. PBX-basierte Telefonie - geschaffen, die moderne Kommunikations- und Kollaborationsfunktionen nicht unterstützen.

Die bestehenden Systeme arbeiten größtenteils in einer unabhängigen Umgebung, die nicht mit dem Internet oder einer Cloud-Infrastruktur verbunden ist.

Während also ein Großteil der Welt vor 10 bis 20 Jahren mit der Umstellung auf die IP-Technologie begann, widersetzte sich der Verteidigungssektor aus einer Vielzahl von Gründen:

- **Sicherheit:** Die Einhaltung gesetzlicher Vorschriften, Datenschutzanforderungen und die Notwendigkeit, sensible Daten zu schützen, machten es schwierig, Technologien einzuführen, die missbraucht werden könnten.
- **Kultur und Führung:** Eine von oben nach unten gerichtete Managementstruktur, die für größere Veränderungsinitiativen eine Genehmigung auf höchster Ebene vorschreibt, bedeutete, dass das Militär den Zustrom von Millennials und Digital Natives aus dem privaten/öffentlichen Sektor verpasste, die einen Druck von unten nach oben erzeugten, um digitale Technologien zu übernehmen.
- **Haushalt:** Angesichts begrenzter Ressourcen hat die Aufrechterhaltung der Einsatzbereitschaft von Ausrüstung und Personal Priorität.
- **Wettbewerb:** Im Gegensatz zur kommerziellen Industrie hat der Verteidigungssektor keine direkten Konkurrenten in der Wirtschaft und konzentriert sich in erster Linie auf die Sicherstellung der technologischen Leistungsfähigkeit von Gefechtsfeldanlagen und vernetzten Kriegsführungssystemen.

Gründe für den Wandel:

Geopolitik und Technologie

Während diese Hindernisse die digitale Transformation behindert haben, hat sich die Welt dramatisch verändert.

Die Pandemie und die geopolitische Instabilität haben gezeigt, wie schnell globale Lieferketten unterbrochen werden können, was erhebliche Auswirkungen auf die lokale Wirtschaft hat.

Und die Geschwindigkeit, mit der sich die Technologie weiterentwickelt, hat Auswirkungen auf die Anforderungen an die Datenverwaltung.

Fortschritte im Bereich des maschinellen Lernens (ML), der künstlichen Intelligenz (KI), fortschrittliche Sensoren und autonome Systeme bilden die Grundlage für eine hochentwickelte und vernetzte Waffengeneration. All diese Technologien spielen eine wichtige Rolle bei den Verteidigungsanstrengungen auf und außerhalb des Schlachtfelds und leiten den Übergang zu einem stärker datenzentrierten Managementprozess im Inland und bei Konflikten ein.

Um die Prozesse zu optimieren und die Einsatzbereitschaft aufrechtzuerhalten, muss jede Verteidigungsorganisation effiziente und effektive Wege finden, um all die zusätzlichen Daten zu erfassen, zu speichern und zu verteilen, die diese neuen Systeme erzeugen.

Bereichsübergreifende Zusammenarbeit

Verschärft wird die Situation durch spezifischere Änderungen des Rahmens, in dem Verteidigungsorganisationen nun arbeiten müssen.

Die traditionellen Abgrenzungen von Luft-, Land- und Seeoperationen sind einer komplexeren globalen Sichtweise gewichen. Um effektiv zu sein, müssen diese unabhängigen Silos nun Teil eines hochgradig vernetzten strategischen Rahmens sein, der sich auf bereichsübergreifende Abläufe konzentriert und auf dem nahtlosen Datenverkehr innerhalb und zwischen allen Bereichen aufbaut.

So hat die NATO beispielsweise ihre traditionellen Operationen zu Wasser, zu Lande und in der Luft um die Bereiche Weltraum und Cyberspace erweitert ( ), um der Datenbedrohung ( ) und der Notwendigkeit einer besseren Abstimmung zwischen diesen Bereichen Rechnung zu tragen.

Noch komplizierter wird dies durch Kooperationsabkommen im Verteidigungsbereich, wie Brandon J. Kinne in seinem Artikel Defense Cooperation Agreements and the Emergence of a Global Security Network schreibt: "...schaffen langfristige institutionelle Rahmenbedingungen für routinemäßige bilaterale Verteidigungsbeziehungen, einschließlich der Koordinierung der Verteidigungspolitik, gemeinsamer militärischer Übungen, Arbeitsgruppen und Ausschüsse, Schulungs- und Ausbildungsaustausch, verteidigungsbezogener Forschung und Entwicklung sowie Beschaffung."[2]

Diese Vereinbarungen beruhen auf neuen operativen Modellen, die auf Informationsaustausch, vernetzten dynamischen Operationen, agiler und schneller Entscheidungsfindung, Echtzeit-Koordinierung und der Notwendigkeit von Informationssicherheit und Ausfallsicherheit basieren.

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

"Innerhalb der NATO-Struktur gibt es fünf Einsatzbereiche: Maritim, Land, Luft, Weltraum und Cyberspace. In der Vergangenheit haben Operationen in diesen Bereichen entweder nicht existiert (z. B. Weltraum und Cyber) oder sie wurden als weitgehend unabhängige Einheiten innerhalb der nationalen Streitkräfte durchgeführt. Die Streitkräfte vieler verbündeter Staaten arbeiten auch heute noch in dieser Eigenschaft; angesichts der Geschwindigkeit des Informations- und Datenflusses und der gegnerischen Fähigkeiten ist es jedoch für langfristige Verteidigungs- und Abschreckungsinitiativen innerhalb der NATO von entscheidender Bedeutung, militärische Aktivitäten in allen Bereichen als eine einzige Streitkraft zu koordinieren."[3]

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

Effiziente und sichere Datenprozesse

Um bereichsübergreifende Operationen zu ermöglichen und die Kooperationsabkommen im Verteidigungsbereich zu unterstützen, benötigen alle Verteidigungsorganisationen Systeme, die einen effizienteren und sichereren Datenaustausch ermöglichen. Daher übernehmen Verteidigungsorganisationen rasch IP -Standards und IoMT-Technologien (Internet der militärischen Dinge) und Systeme, um der Notwendigkeit Rechnung zu tragen, immer mehr kontextbezogene Daten an Bord von Schiffen, Fahrzeugen und unbemannten Objekten sowie als Wearables für unterstützte Soldaten zu erfassen und zu verarbeiten.

Doch während IoMT-Technologien Daten sammeln können, ist es immer noch eine Herausforderung, diese Daten effizient zu liefern, zu verteilen und zu verarbeiten. Infolgedessen erwägen viele Verteidigungsorganisationen jetzt , wie sie ihre Prozesse am besten optimieren können, indem sie unabhängige Systeme der Betriebstechnologie (OT) und der Informationstechnologie (IT) in einem konsolidierten Betriebsrahmen zusammenführen.

Darüber hinaus hat die Weiterentwicklung und Verfeinerung der Technologie es den Staaten ermöglicht, eine effizientere Cyberkriegsführung zu betreiben. Daher muss der Umfang der Verteidigungsbemühungen nun auch digitale Abschreckungsfähigkeiten gegen Cyberangriffe auf kritische Infrastrukturen sowie gegen Fehlinformations-, Desinformations- und schadinformationskampagnen umfassen.

Mit veralteten und überholten IKT-Systemen ist das natürlich nicht zu machen. Noch wichtiger ist, dass veraltete und überholte Systeme nicht in der Lage sind, multidisziplinäre Operationen zu unterstützen, die auch den Cyberbereich einschließen. Sie können auch keine Kooperationsvereinbarungen mit Partnerländern im Verteidigungsbereich unterstützen, die Informationen austauschen und sicher sein müssen, dass diese Informationen geschützt und sicher sind.

Anwerbung und Bindung von Mitarbeitern

Der Verteidigungssektor steht vor denselben Herausforderungen, mit denen sich Wirtschaftsunternehmen tagtäglich auseinandersetzen müssen: Wie lassen sich Spitzenkräfte anwerben und binden? Die Verteidigungsorganisationen müssen über IKT-Instrumente verfügen, um das Personal in allen Bereichen zu schulen, ein effizientes und lohnendes Arbeitsumfeld zu schaffen und die Vereinbarkeit von Beruf und Privatleben zu ermöglichen, die die Mitarbeiter heute erwarten.

"...eine wirklich vernetzte Organisation wird die Integration auf nationaler und internationaler Ebene in allen fünf Bereichen ermöglichen: Maritim, Land, Luft, Cyber und Weltraum. Dies wird es dem Verteidigungsbereich ermöglichen, die Leistungsfähigkeit seiner Daten voll auszuschöpfen und Sensoren, Entscheidungsträger und Effektoren in großem Umfang und mit hoher Geschwindigkeit zu verbinden."[4]

BRITISCHES VERTEIDIGUNGSMINISTERIUM

4 - "Data Strategy for Defence: Delivering the Defence Data Framework and Exploiting the Power of Data", britisches Verteidigungsministerium, September 2021.

Lehren aus dem öffentlichen/privaten Sektor

Diese externen Faktoren sind zwar allesamt Triebfedern für den Wandel, doch viele Verteidigungsorganisationen setzen Strategien zur digitalen Transformation nur langsam um - obwohl sich die digitale Transformation sowohl für öffentliche als auch für private Unternehmen als wirksames Mittel zur Steigerung der Effizienz und zur Verbesserung der Abläufe erwiesen hat. Und da viele Beschäftigte im Verteidigungsbereich nicht im Kampfeinsatz sind, gelten die Ansätze zur Umgestaltung und die daraus gezogenen Lehren auch für Gebäude der Verteidigungsverwaltung und Militärbasen.

Auch die IKT-Technologien sind inzwischen so weit ausgereift, dass viele der technologischen Probleme der Vergangenheit kein Thema mehr sind. Es stehen kostengünstige, einfach zu implementierende digitale Lösungen zur Verfügung, die auf Standardprotokollen beruhen und digitale Verteidigungsarbeitsplätze mit effizienter Kommunikation und Zusammenarbeit unterstützen können. Und viele bieten das hohe Maß an Cybersicherheit, das Unternehmen benötigen.

Die strategische digitale Transformation wird die Verteidigungsorganisationen in die Lage versetzen, die neue Realität, in der sie operieren, besser zu bewältigen. Eine wirksame Umgestaltung schafft ein sicheres digitales Umfeld, in dem alle verfügbaren Daten schneller und sicherer bewegt werden können, um die Mitarbeiter in allen Bereichen zu unterstützen und zu befähigen. Und um dieses Umfeld zu schaffen, können Verteidigungsorganisationen bewährte Ansätze zur digitalen Transformation aus dem privaten und öffentlichen Sektor anwenden.

Im nächsten Abschnitt werden wir untersuchen, welche Erfahrungen bei der Umsetzung von Strategien zur digitalen Transformation im öffentlichen/privaten Sektor gemacht wurden und wie sich diese auf Verteidigungsorganisationen übertragen lassen.

Intelligente Gebäude und hyperintelligente Infrastruktur

Intelligente Gebäude sind mittlerweile Bestandteil von Stadtzentren auf der ganzen Welt und können problemlos in Verteidigungsverwaltungszentren und Militärstützpunkten errichtet werden. Diese Gebäude nutzen IoT-Technologien zur intelligenten Überwachung und Verwaltung von Beleuchtung und Heizung bis hin zu Überwachungssystemen an wichtigen Ein- und Ausgängen.

Die kontinuierliche Weiterentwicklung der IoT-Technologien hat es ermöglicht, extrem aufmerksame Infrastrukturen zu schaffen. Diese digital vernetzten Strukturen kombinieren Betriebsautomatisierung mit kontextbezogenem Raummanagement, um den Betrieb des Gebäudes auf intelligente Weise an die Verkehrsmuster in Schlüssel-bereichen sowie an die Komfort- und Sicherheitsbedürfnisse der Bewohner und der Umgebung anzupassen. Das Ergebnis sind intelligente Räume, die den Arbeitsplatz sicherer, gesünder und zufriedener machen, die Erfahrung der Mitarbeiter verbessern und die Produktivität steigern.[5]

Intelligente Stadtkonzepte

Da Militärstützpunkte eigenständigen Städten ähneln, sind intelligente Gebäude und extrem aufmerksame Infrastrukturen wichtige Bestandteile bei der Schaffung intelligenter Stützpunkte, die auf bewährten Smart-City-Konzepten aufbauen.

Intelligente Stützpunkte nutzen die auf einem Stützpunkt verfügbaren Daten und schaffen "eine sichere intelligente Infrastruktur, energieeffiziente Gebäude, effiziente Verkehrsmittel, kosteneffiziente Betriebsabläufe und eine höhere Lebensqualität für die Einwohner"[6]

Die Netzinfrastruktur, die einen intelligenten Stützpunkt ermöglicht, kann auch dazu genutzt werden, eine effektivere Sicherheitsstruktur zu schaffen, die nicht nur die Daten in der Basis, sondern auch die physische Sicherheit von Personal und Einrichtungen schützt. Dies kann mit fortschrittlichen Sicherheitssystemen erreicht werden, wie z. B. der Perimeter-überwachung und Einbruchserkennungssystemen, die mit IoT- und KI-Lösungen in Verbindung mit Sicherheitszentren erstellt wurden.

Die Schaffung intelligenter Grundlagen geht über die Installation der neuesten Sensoren und Systeme hinaus. Es geht darum, alle bestehenden und neuen Technologien und Prozesse in einen kohärenten IKT-Netzrahmen zu integrieren, der auf den modernsten Technologien aufbaut und durch eine strategische digitale Transformation umgesetzt wird.

Und dieser Wandel lässt sich auch auf andere Bereiche übertragen, wie z. B.:

- Feldeinsätze, bei denen IKT-Technologien als Rückgrat der Informationsnetze auf militärischen Schiffen und Fahrzeugen und als Bindeglied für einen vernetzten Kämpfer eingesetzt werden, der hochentwickelte tragbare Sensoren und Geräte nutzt
- Kommando- und Kontrollzentren, in denen IKT-Technologien die Unterstützung von Zivilschutzmaßnahmen oder das Krisenmanagement mit anderen staatlichen Stellen bei Naturkatastrophen erleichtern

Die Macht der modernen IKT

Mit den modernsten IKT-Technologien werden die Verteidigungs-organisationen besser in der Lage sein, Informationen auszutauschen, Strategien zu koordinieren und gemeinsame Operationen überall durchzuführen.

Der Schlüssel zu einer effektiven digitalen Transformation ist ein zweckmäßiger strategischer Kommunikations- und Netzwerkrahmen, der für den intelligenten Stützpunkt optimiert ist.

Dieses Netz muss sicher, robust und so ausgelegt sein, dass es jederzeit alle Verbindungen unterstützt, um große Datenmengen effizienter zu übertragen. Und sie muss mit IKT-Lösungen aufgebaut werden, die die Integration und Vernetzung von Verwaltungsabläufen, Militärstützpunkten, Einsatzkräften und -mitteln zu Lande, in der Luft, zur See und im Weltraum sowie die Eindämmung von eskalierenden und schädlichen Bedrohungen aus dem Cyberspace unterstützen.

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

ALE: Ein Partner für die digitale Transformation

Alcatel-Lucent Enterprise kennt die Herausforderungen, denen sich Verteidigungsorganisationen bei der Planung und Entwicklung von Strategien zur digitalen Transformation stellen müssen, die IKT-Technologien nutzen, um die Anforderungen des heutigen Militärs zu erfüllen.

ALE unterstützt die digitale Transformation mit robusten und sicheren Lösungen für die vernetzte Verteidigung, einschließlich:

- IoT-fähige LAN und WLAN Lösungen, inklusive robuster Switche, die Netzwerkanforderungen erfüllen und ein sicheres und automatisiertes IoT-Onboarding für eine Vielzahl von vernetzten Verteidigungsanforderungen bieten
- Kommunikations-, Kollaborations- und CPaaS-Lösungen, die vor Ort, cloudbasiert oder in einem Hybridmodell bereitgestellt werden können
- Lösungen zur Workflow- und Prozessautomatisierung, die durch Monitoring Probleme proaktiv erkennen und beheben, bevor sie sich auswachsen, was die betriebliche Effizienz steigert und Kosten senkt
- Sicherheit durch „Privacy by Design" auf der Grundlage eines Zero-Trust-Prinzips, mit allen relevanten Datenschutzzertifizierungen in den Ländern, in denen wir tätig sind

ALE-Kommunikations- und Netzwerklösungen können optimiert werden, um redundante Architekturen zu schaffen, die jeden und alles in einem zusammenhängenden, vollständig integrierten und hochverfügbaren Rahmen verbinden.

Darüber hinaus sind unsere Lösungen auf höchste Sicherheit ausgelegt. Wir halten uns strikt an die aktuellen Sicherheitspraktiken und -standards und integrieren eine Reihe von verwandten Technologien ohne zusätzliche Kosten in unsere Produkte. Sicherheit basiert auf einem mehrschichtigen Ansatz, der Netzwerkintegrität, Gerätesicherheit und Zugriffsrichtlinien auf der Grundlage von Benutzerprofilen und Anwendungssichtbarkeit umfasst. Netzsoftware wird durch die Validierung des zugrunde liegenden Codes durch Dritte überprüft. IoT-Systeme und Benutzer werden automatisch und sicher an Bord genommen und in Containern platziert, die so strukturiert sind, dass potenzielle Cyberangriffe von einem kompromittierten Gerät abgehalten werden. Und alle Daten und Kommunikationen werden mit starken Verschlüsselungsmechanismen verschlüsselt, um Abhör- und Man-in-the-Middle-Angriffe zu verhindern.

Für zusätzliche Sicherheit erfüllen unsere Lösungen auch die strengsten Sicherheitszertifikate, die von unabhängigen Organisationen und staatlichen Einrichtungen ausgestellt werden.

Und unser Rahmenwerk Risk, Resilience and Security (RRS) befasst sich mit Cyber- und physischer Sicherheit für den Regierungs- und Verteidigungssektor.

Wir wissen auch, wie wichtig die Datensouveränität ist. Unsere Cloud-basierten Anwendungen bieten flexible Hosting-Optionen - in fortschrittlichen und hochsicheren Rechenzentren, die für eine schnelle und zuverlässige Leistung sorgen, oder vor Ort mit unserer privaten Cloud-Lösung Rainbow Edge. Die in der Cloud gespeicherten Daten sind Eigentum unserer Kunden, und wir geben keine Daten an andere Unternehmen oder Länder weiter oder verkaufen sie.

Weitere Informationen

Wenn Sie mehr über die Lösungen von Alcatel-Lucent Enterprise für die Verteidigungsindustrie erfahren möchten, besuchen Sie unsere Website oder kontaktieren Sie uns, um zu besprechen, wie wir Sie bei der Entwicklung einer auf Ihre Verteidigungsorganisation zugeschnittenen Strategie für die digitale Transformation unterstützen können.

Alcatel·Lucent
Enterprise