bitkom

# Steckbrief Cloud im Militär

PG Innovationen AK »Verteidigung« Bitkom | Stand September 2023

Thema: Multicloud im Militär

## Cloud: Ausgangssituation und Beschreibung der Technologie

- Ausgehend von den Geschäftsmodellen des Outsourcings, zur Verringerung der betriebsrelevanten Fertigungstiefe, haben sich seit den 2000er Jahren diese auch für den Bereich der IT Verlagerungen etabliert. Dies begann mit Infrastruktur und infrastrukturnaher Maintanance und erweitere sich auf Software und »Dienstleistung-as-a-service«-Modelle.
- Die öffentliche Hand war hier bisher äußerst restriktiv in der Adaption, da sie nicht Geschäftsmodellgetrieben agiert. Das galt auch für den Bereich der Verteidigung. Vielmehr war das Paradigma gültig, dass Verarbeitung, Übertragung und Speicherung von Daten nur dann sicher ist, wenn sie vollständig im »eigenen« Haus stattfindet.
- Im Besonderen unterliegen die Cloud-Angebote der Industrie bzw. der Hyperscaler einer Zulassungshürde zur Verarbeitung von eingestuften Informationen. Dies wird in Zukunft weiterhin durch die Vorgaben des Bundesamtes für Sicherheit und Informationstechnik (BSI) geprägt sein. Sollten einzelne Anbieter eine Zulassung zur Verarbeitung von Daten der Einstufung »VS-NUR FÜR DEN DIENSTGEBRAUCH« nachweisen können, so ist eine schnelle Erweiterung der Nutzung für zumindest Verwaltungsaufgaben im Geschäftsbereich des Bundesministeriums für Verteidigung (BMVg) zu erwarten. Für die Verarbeitung von Daten im Zusammenhang mit einer militärischen Operationsführung bzw. die einem Geheimschutzinteresse unterliegen, sind diese Hürden noch einmal von einem tiefen Einblick in die eigentliche Technologie der Anbieter abhängig.
- Bei allen weiteren Betrachtungen zur sinnvollen Nutzung der Cloud – quasi als conditio sine qua non – ist innerhalb des Geschäftsbereichs der Verteidigung das Geschäftsmodell und damit die Nutzungsdimension des »Warum und wofür?« zuallererst festzulegen. Das klingt banal, aber das »Warum« also die Wirtschaftlichkeitsberechnung, fehlt bisher weitestgehend. Dabei ist aber auch zu beachten, dass es aus militärischer Sicht weniger um eine Wirtschaftlichkeitsbetrachtung geht, sondern um die resiliente Bereitstellung von IT-Services. Dazu gehört, dass einheitliche Plattformen auf unterschiedlichen Ebenen genutzt werden können, diese skalierbar und schnell wiederherstellbar sind und, dass die vorhandenen Grundkomponenten »Compute – Storage – Networking« zu einer modularen und flexiblen Plattform als Infrastructure-as-a-Service (IaaS) zusammengebunden werden.
- Erste konzeptionelle Überlegungen KdoCIR bzw. ZDigBw sind es, dass im Ansatz »Multicloud Bundeswehr« eine eigene Cloud Architektur (pCloudBw) auf eigenen Rechenzentren (RZ) betrieben wird. Darüber hinaus aber weitere Plattformen der Ebene IaaS bis Platform-as-a-Service (PaaS) durch andere Provider des Bundes, der NATO, Europäischen Union (EU) und auch ziviler Betreiber (sogenannte Hyperscaler bzw. kleinere Anbieter wie z. B. Microsoft, AWS, Google, Oracle, Ionos, StackIT etc.) genutzt werden. Dabei soll

in Zukunft auf der Applikationsebene sichergestellt werden, dass wichtige IT-Services auf mindestens zwei Plattformen lauffähig sind.

**Treiber der Cloud:**

- Der technologische Fortschritt, insbesondere die bessere Vernetzung, ermöglicht neue Innovationen im Bereich der IT-Dienstleistungen und Anwendungen. Diese können als Cloud-Services angeboten werden und militärische Fähigkeiten durch IT-Unterstützung der Bundeswehr und die Führungsüberlegenheit durch Informationsvorsprung nachhaltig verbessern.
- Die Komplexität im Aufbau und Betrieb von IT-Infrastrukturen steigt und wird immer schwerer beherrschbar. Fehlende Fähigkeiten und Fachkräftemangel zwingen viele Organisationen, damit verbundene Aufgaben an externe Dienstleister zu vergeben. Diese Entwicklung trifft die Bundeswehr ungleich stärker.
- Die allgemeine Marktentwicklung treibt den Ausbau von Cloud-Lösungen (getrieben von den großen Technologiekonzernen). Konsum- und Lizenzierungsmodelle werden daraufhin ausgerichtet, innovative Lösungen und Weiterentwicklungen werden nur noch als Cloud-Service angeboten. Dadurch wird das Angebot von On-Premises-Lösungen geschwächt. Die Bundeswehr hat keinen Hebel diese Entwicklung aufzuhalten und muss diese Entwicklung mitgehen, um konkurrenzfähig zu bleiben.
- Cloud-Provider können in ihren hochgerüsteten RZ teilweise ein höheres Maß an Datenresilienz und Datensicherheit garantieren als es in manchen RZ der Wirtschaft und öffentlichen Verwaltung der Fall ist. Um eingestufte Daten in einer Cloud speichern und verarbeiten zu können, ist jedoch die Zulassung der Plattform (IaaS/PaaS) und die damit einhergehende Freigabe der Cloud-Infrastruktur durch das BSI oder das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) nötig.
- Technologische Entwicklungen wie Künstliche Intelligenz (KI), 5G-Netzwerke, Konnektivität oder Zero Trust Networks sind ohne Cloud nicht denkbar und benötigen zum Teil sehr große Rechenleistung, was in den kleinen RZ-Infrastrukturen der Bundeswehr nie wirtschaftlich und nachhaltig umgesetzt werden kann.
- Die sicherheitspolitischen Entwicklungen verlangen eine georedundante Bereitstellung von Plattformen und der darauf zu verarbeitenden Daten, auch im Zuge eines Krisenfalles, aber auch die Interoperabilität mit Partnern, um z. B. Daten und Applikationen zu teilen (Bsp.: Ukraine hat ihre Daten mit Erfolg in die Cloud verlagert, um auch bei der physischen Vernichtung von RZ einsatzbereit zu sein). Allerdings ist hierbei die Vernetzung der einzelnen Zonen bzw. Regionen ein deutlicher Schwachpunkt. Es ist davon auszugehen, dass weitreichende Anbindungen bzw. Seekabel gestört oder gar zerstört werden.
- Die Folgen des demografischen Wandels erfordern zunehmend Einsparungen bei Kosten, Ressourcen und Personal.
- Es besteht ein Bedarf und Möglichkeiten der Echtzeit-Verarbeitung von Daten (Verwaltung & Gefechtsfeld).
- Die Cloud bietet die Chance zur Professionalisierung und Spezialisierung auf einsatzrelevante Funktionen (IT-Infrastruktur muss nicht mit eigenen Bundespersonalressourcen betrieben werden)

**Vorteile der Cloud:**

- ermöglicht Agilität und Skalierung (schnelle Bereitstellung von neuen, standardisierten Services, bzw. zeitnahe Skalierbarkeit
- Updates von Plattformen im Rahmen von Software Defined Defense werden im Backend vorbereitet und dann bis in die einzelnen Waffensysteme bei Verfügbarkeit einer Anbindung ausgerollt.
- Integration von innovativen Services wie z. B. KI, Blockchain, Smart Dust, Digital Twin, usw. Dabei ist jedoch, wann immer möglich, ein Anteil dieser Technologie im System des Edge-Bereiches (z. B. Drohnen, Aufklärungssysteme) zu halten. Es kann nicht immer garantiert werden, dass ein Bild zur Auswertung in die »große Cloud« gesendet werden kann. Diese Anbindung ist als oft gestört oder unterbrochen anzunehmen. Das Anlernen der modernen Technologien wie z. B. KI kann jedoch in den großen Clustern stattfinden.
- Interoperabilität durch Technologieoffenheit auf Basis einer von der Bundeswehr definierten Plattform (IaaS, PaaS), auf die sich alle »aufschalten« müssen. Dabei erstreckt sich diese Plattform auf einen »Cloud Core« in stationären RZ bzw. mit hybriden Anteilen aus militärischen und zivilen/industrielle Cloud-Elementen über den Bereich »Fog« (verlegefähige RZ) bis zum Endgerät/Waffensystem im »Edge«.
- Kosteneffizienz gegenüber stationären Lösungen wie eigenen RZ kann entstehen (Kosteneffizienz entsteht durch die Skalierbarkeit der Ressourcen. Die RZ werden überwiegend weiter Bundeswehr-RZ sein oder von der Bundeswehr angemietete RZ).
- IT-Standards sowie Sicherheit durch Provider und damit Resilienz (Herausforderungen u. a. durch: Cybervandalismus, Insider Threats innerhalb der Organisation, Serviceunterbrechungen, Cyberangriffe) werden verbessert.
- Service-Orientierung (Software-as-a-Service, SaaS) wo Nutzenden eine Webanwendung mit all ihren zugrunde liegenden IT-Infrastrukturen und -Plattformen zur Verfügung gestellt wird. Dies erfolgt insbesondere dann, wenn die Infrastruktur, Plattformen und Software nicht selbst verwalten sollen oder wenn man z. B. Software-Subskriptionen bevorzugt. Somit lassen sich Vorabkosten reduzieren, da andauernde Softwareanschaffungen oder Investitionen in eine robuste lokale IT-Infrastruktur ausgelagert sind.
- Platform-as-a-Service (PaaS), auf der eigene Apps entwickelt, ausgeführt und verwaltet werden können, ohne die dafür notwendige Infrastruktur oder Umgebung entwickeln und pflegen zu müssen. Denn bei PaaS wird den Nutzenden die Hardware und die Softwareplattform eines Drittanbieters oder einer zentralen Instanz zur Verfügung gestellt. Das heißt, Nutzende kontrollieren nur die tatsächlichen Anwendungen und Daten, die sich auf der Plattform befinden. Das macht PaaS zur idealen Lösung für Entwickler und Programmierert. So kann z. B. ein Entwickler PaaS als Basis verwenden, um eine neue Anwendung zu erstellen, die in eine bestehende Datenbank eines Unternehmens integriert werden kann.
- Infrastructure-as-a-Service (IaaS) wo die Infrastruktur (z. B. Server, Netzwerk, Virtualisierung und Storage) für Anwendende von einem Anbieter über eine Public Cloud oder eine Private Cloud gemanagt wird. Nutzende greifen über eine Programmierschnittstelle (API) oder ein Dashboard auf diese Infrastruktur zu. Dabei können für die Nutzerin bzw. den Nutzer transparent unterschiedliche Plattformen zum Einsatz kommen. Diese können eigene Rz-Infrastrukturen sein oder hybride Elemente aus anderen Plattformen der Industrie. Dabei können Komponenten wie Betriebssystem, Apps und Middleware verwaltet werden,

während der Anbietende (Bundeswehr/Industrie) Hardware, Networking, Festplatten, Storage und Server bereitstellt und für jegliche Ausfälle, Reparaturen und Hardware-Probleme verantwortlich ist.

- Keine operativen Aufwände zum Aufbau, Betrieb, Pflege und Weiterentwicklung der Infrastruktur

**Nachteile der Cloud**

- Keine Offline-Fähigkeit von Public- oder Hybrid-Cloud-Modellen: durchgehende Vernetzung und sicherer Zugriff sind bindend. Hier kann mit Synchronisierungs-Modellen / -Architekturen entgegengewirkt werden.
- Cloud erfordert einen sehr hohen Standardisierungsgrad – bietet dafür Geschwindigkeit, Sicherheit und vor allem Interoperabilität.
- Ein verändertes IT-Betriebsmodellerfordert Umdenken aller Beteiligten entlang der Wertschöpfungskette. Neue Rollen und organisatorische Umstrukturierungsmaßnahmen sind unmittelbar mit einer erfolgreichen Cloud-Strategie verknüpft.
- Neue Sicherheitsstrategien zum Schutz der Informationen sind notwendig (z. B. Zero Trust). Das Ziel einer Multi-Level-Security-Cloud zur Verarbeitung unterschiedlich eingestufter Daten auf derselben Hardware ist noch nicht erreicht und der Aufwand zur Entwicklung einer solchen Lösung ist sehr aufwändig.
- Die Nutzung offener Standards zur Vermeidung eines Vendor lock-ins ist nicht bei allen Cloud Angeboten gegeben.

## Gemeinsames Ziel/Nutzungspotenziale/ Cloud-Verständnis

- Das Cloud-Computing-Betriebsmodell schafft über den einheitlichen Plattformgedanken, d. h. einer einheitlichen Abstraktionsebene, auf der Anwendungen ausgeführt und entwickelt werden können, die Voraussetzung für Standardisierung, Automatisierung und Interoperabilität von IT-Leistungen. Die Nutzerin, der Nutzer oder die Anwendung interagiert nur mit der einheitlichen Plattform. Die darunter liegende Infrastrukturebene ist für die Anwenderin bzw. den Anwender unsichtbar. Die Infrastruktur kann unterschiedlich aufgebaut sein, von unterschiedlichen Anbietern kommen oder unterschiedliche Technologien beinhalten. Darüber hinaus ist sie austauschbar, ohne dass die Nutzerin, der Nutzer oder die Anwendung dies mitbekommt.
- Bei konsequenter Einhaltung des Schichtenmodells einer Cloud-Infrastruktur (Infrastruktur, Virtualisierungsplattform, Anwendungsplattform, Anwendungen) sind alle Schichten austauschbar, solange auf eine Verflechtung der Schichten verzichtet wird, um eine gegenseitige Abhängigkeit zu vermeiden. Dadurch werden Vendor lock-in Effekte vermieden sowie die Digitale Souveränitätsstrategie der öffentlichen Verwaltung unterstützt und auf die Bundeswehr ausgeweitet.
- Des Weiteren ermöglicht ein Cloud-Betriebsmodell über die einheitliche Abstraktionsebene die Umsetzung gleicher Betriebsverfahren und -prozesse, d. h. Interoperabilität, über die unterschiedlichen Einsatzformen in der Bundeswehr hinweg: stationär, verlegefähig, mobil, Edge.

- Die Einführung einer Service-orientierten Architektur (SOA), als fester Baustein der Digitalisierungsstrategie der Bundeswehr, ist Grundvoraussetzungen für eine Cloud-Computing-Strategie. Cloud-Computing ist gleichzeitig Antwort für die technologische Umsetzung einer SOA.
- Anwendungen und Services können entwickelt oder beschafft werden, ohne das vollständige »Silo« (alles, was für den Betrieb der Anwendung notwendig ist) mit in die Betrachtung einzubeziehen. Der Entwickler oder Lieferant der Anwendung oder des Services erhält klar definierte Rahmenvorgaben bzw. Standards und wird ggf. vertraglich dazu gebunden, auf der ausgewählten Plattform die Applikation zu entwickeln. Das Produkt kann dann unabhängig von der Infrastruktur oder dem Standort überall in Betrieb genommen werden, wo die Abstraktionsebene existiert. Dadurch können neue Lösungen viel schneller umgesetzt und Kosten eingespart werden. Ausschreibungen werden schlanker und beinhalten weniger Abhängigkeiten. Darüber hinaus wird die Vielfalt unterschiedlichster Komplett-Lösungen innerhalb der Bundeswehr reduziert. Es ist damit zu rechnen, dass dadurch weniger Unterstützungsleistung eingekauft werden muss und sich die Anforderungen an die Breite der operativen Fähigkeiten und Skills beim IT-Betriebspersonal reduzieren. Lieferanten der Rüstungsindustrie können sich auf die digitalen Mehrwerte ihrer Lösung konzentrieren, anstatt sich zusätzlich um den Aufbau einer Betriebsplattform zu kümmern.
- Ebenso liefert das Plattform-Konzept mit der Abstraktionsebene die Fähigkeit, nach dem »Lift-and-Shift«-Prinzip Anwendungen zu verschieben, zu evakuieren oder bei Verlust der Laufzeitumgebung an einem anderen Ort wieder in Betrieb zu nehmen. Ziel dabei muss es sein, dass mindestens immer zwei unterschiedliche Plattformen zur Verfügung stehen. Zusätzlich lassen sich Anwendungsarchitekturen umsetzen, deren Laufzeitumgebung sich nicht nur auf einen Cloud-Standort beschränkt, sondern standortübergreifend, hochverfügbar, redundant und damit resilient aufgebaut werden.
- Die Verwendung von Virtualisierungstechnologie in Cloud Infrastrukturen vereinheitlicht unterschiedlichste Hardware-Lösungen heterogener Hersteller und Zulieferer zu einer homogen Software-definierten Betriebsumgebung (bzw. Plattform). Infrastrukturleistungen können über eine einheitliche Schnittstelle (API) angefragt und bereitgestellt werden. Mithilfe dieser Eigenschaften ist eine durchgehend automatisierte und reproduzierbare Inbetriebnahme von Services inklusive der benötigten virtuellen Infrastruktur möglich (Infrastructure as Code). Des Weiteren können in der physischen Infrastruktur unterschiedliche Hardware-Lösungen (Compute, Networking, Storage etc.) zum Einsatz kommen, ohne diese Schnittstelle zu verändern. Dadurch können Automatisierungsabläufe zur Bereitstellung von Cloud-Services agnostisch genutzt werden, d. h. Cloud-übergreifend, bzw. ohne die zugrundeliegenden Details der genutzten Cloud Infrastruktur zu kennen (Interoperabilität).
- Bereitstellung von Cloud-Technologien, entweder On-Prem im Bundeswehr-RZ oder aus einem sicheren RZ eines externen Anbieters oder Public Cloud Lösungen (Hyperscaler, souveräne Cloud Lösungen, ...).
- Auf der »Multicloud Bundeswehr« (MultiCloudBw) (hier als Sammelbegriff für die nutzbaren Cloud-Alternativen genutzt) werden künftig alle Services (soweit nicht aus Gründen der IT-Sicherheit, Einstufung etc. etwas dagegenspricht) bereitgestellt, die für den Landes- und Bündnisfall sowie im Friedensbetrieb, sowohl im In- und Ausland notwendig sind.
- Die »Multicloud Bundeswehr« muss eine Interoperabilitätsschicht (von der Bundeswehr definiert) bereitstellen, über die eine Unabhängigkeit von der darunter liegenden HW-Infrastruktur sichergestellt wird.

Nur so kann die Idee, Services beliebig zwischen den einzelnen Komponenten einer MultiCloudBw verschieben zu können, realisiert werden. Gleiches gilt für die Realisierung des »neuen« Paradigmas Software Defined Defense (SDD). Services müssen auf einem Tank-OS ebenso betrieben werden können wie auf dem Fighter-OS oder Ship-OS.

- Ziel muss eine Lösung sein, mit der auf einer IT-Infrastruktur alle relevanten Sicherheitsdomänen nebeneinander BSI-konform betrieben werden können (ohne massiven Hardwareoverhead | physische Trennung). Dabei gilt es jetzt schnell eine Technologieführerschaft zu erreichen, die es ermöglicht unterschiedliche Sicherheitsdomänen auf einer einheitlichen Plattform zu ermöglichen.
- Trennung grüner und weißer IT ist nicht mehr möglich. Zukünftig sollen alle Applikationen in der Cloud betrieben werden, sodass dort alle Lösungen bereitgestellt werden.
- Die Cloud soll im Verteidigungs- und Bündnisfall genutzt werden sowie im Friedensbetrieb, sowohl im In- als auch im Ausland.
- Die Interoperabilität soll durch Abbau von spezifischen Lösungen (Joint & Combined) und einer strengen Ausrichtung der Vorgaben aus dem »Federated Mission Networking (FMN)« für die Hardware- und Softwareschicht gesteigert werden. Hier kann die Bundeswehr in den Gremien der NATO und mit Unterstützung der Industrie die Vorgaben FMN nachhaltig gestalten.
- Die Entscheidungsfähigkeit soll durch umfassende, zeitnahe Informationen (Auswertung, Gewinnung, Verteilung) optimiert werden.
- Durch technische Unabhängigkeit (Rollouts, Daten- und Infrastrukturbereitstellung und Services) werden
- Agilität und Flexibilität verbessert. Eine Dezentralisierung von Entscheidungen wird durch ein umfassendes Lagebild möglich.
- Außerdem besteht ein Zugriff von jedem Ort und zu jeder Zeit (Voraussetzung: Datenverbindung).

## Mögliche Anwendungsfelder in der Bundeswehr

**Ausbildung**

- Grundlage für den Betrieb digitaler Zwillinge und anderer Applikation mit großen Datenmengen (z. B. Marine virtuelles Training)
- Schulungen
- verbessertes digitales Lernen & Entwicklungsfähigkeiten
- Infrastruktur
- Gebäudeplanung mit dem Building Information Model
- Gebäude und Flächenmanagement

**Betrieb**

- Development Security and Operations (DevSecOps) Integration von Sicherheitsaspekten als zusätzliche Komponente in die vorhandenen Entwicklungs- und Unternehmensprozesse
- CI/CD für eine nahtlose und automatisierte Bereitstellung sowie Orchestrierung von Cloud-Services
- Realisierung digitales Gefechtsfeld (bedingt durch Sensorik, Führungsinformationssysteme – virtuelle Lagebilder)
  - granulare Vernetzung von umfassendem Lagebild: Informationen in Echtzeit an entsprechende Einheiten, Systeme, Waffen, Netzwerke versenden (Arbeitsstichwort)
- cloudbasierte Nutzung von Applikation und Informationsverteilung zum Aufbau eines einheitlichen Lagebildes und Situational Awareness im NATO-Verbund
- Lagebilder in der Zivil-militärischen-Zusammenarbeit durch Bereitstellung gemeinsam nutzbarer Ressourcen (Polizei, Feuerwehr, Technisches Hilfswerk und weiterer Akteure im Katastrophenschutz (KVInfoSysBund)
- Logistik: Lifecycle-Management, z. B. bei Fahrzeugflotten | Optimierung Logistikketten | Instandhaltung von Fahrzeugen, Schiffen und Flugzeugen | digitaler Zwilling | automatisierte Inspektion
- Wartung mit Predictive Maintenance
- Auswertung Satellitenbilder
- Übersetzungsservices bei mobilen Anwendungen
- Rechenleistung in gehärteter Umgebung (temporär nahe Gefechtsfeld, z. B. Gebäude | Standort Edge)
- Rechenleistung in großen mobilen Plattformen (Schiffe, Flugzeuge | große Mobile Edge)
- Rechenleistung in kleinen Plattformen (Fahrzeuge etc. | Netzwerk kleine Mobile Edge)
- Intelligence &Analytics: automatisierte Datenerfassung | Verarbeitung großer Datensätze | Erkennung von Mustern / Anomalien | Einsatz von neuen Technologien: Künstliche Intelligenz/ Machine Learning
- Operations: automatisieren und sammeln von Sensordaten | Echtzeit-Datenanalyse | höhere Flexibilität und dynamische Reaktionsfähigkeit in Echtzeit | Edge-Computing
- VR/AR-Support
- Datentriangulation
- Überwachung der SB/MSB durch softwareunterstützte Sicherheitssysteme, die in der Cloud Bilder und Sensordaten auswerten; somit Unterstützung des zivil- und militärischen Wachpersonals
- Product Lifecycle Management auf Grundlage großer Datenmengen zur Vorhersage von Ausfällen

**Personal**

- Sanitätsdienst – Gesundheitsdatenanalyse
- Personalplanung
- Moderne HR-Services für die zivile sowie militärische Belegschaft (Bundeswehr Messenger, Laufzettel, Personalakte, Abrechnungen, Urlaub, Seminare etc.)
- Berufsförderungsdienst
- Verbessertes Personal-Management
- Durchführung von HR-Analysen

**Organisation**

- Cybersicherheit/ Bedrohungserkennung durch Applikationen in der Cloud (Malwareanalyse | Verwundbarkeitsmanagement | Angriffsoberflächenmanagement etc.) | Defense Security Operations | Echtzeit-Bedrohungsanalyse | verbesserte Erkennung von Schatten-IT-Nutzung | Erhöhung der Sicherheitsreaktionen | volle Sichtbarkeit des Benutzers
- Aufbau eines 5G-Campusnetzwerkes
- Trainieren von KI-Modellen
- Vernetzung vorhandener Daten und Nutzung mittels KI
- Analyse sensibler Datensätze
- Skalierbares Intranet
- IoT basierte $CO^2$-Optimierung im Geschäftsbereich BMVg
- Vernetzung von Organisationseinheiten, Dienststellen und Prozessen
- Der Betrieb einer sicheren Cloud-Infrastruktur für den Einsatz nahe dem Gefechtsfeld und im Gefechtsfeld auf mobilen Plattformen im Multi-Domainansatz im Bereich Edge und Fog, um den Aufbau eines System of Systems durch die Integration und Nutzung unterschiedlicher IT-Services unterschiedlicher Hersteller zu einem flexiblen Gesamtsystem zu gewährleisten. Dadurch wird eine Leistungssteigerung im Bereich Aufklärung und Wirkung erzielt und auch mittels KI-gestützte Entscheidungsfindung Prozesse beschleunigt.
- Standardisierung, Automatisierung, Interoperabilität:
- Cloud-Computing setzt ein hohes Maß an Standardisierung voraus. Der Zugriff auf Ressourcen und Funktionalitäten einer Cloud wird über Application Programming Interfaces (APIs) realisiert. Beides erlaubt eine umfassende Automatisierung von Abläufen, ermöglicht die nahtlose Integration von Cloud-Services in bestehende Services, ermöglicht die Interaktion verschiedener Cloud-Plattformen über gemeinsame Standards und fördert die Interoperabilität.
- Kollaboration: Zusammenarbeit und Kommunikation in Echtzeit; Austausch von Informationen und Daten durch gemeinsamen, ortsunabhängigen Datenzugriff
- Datenverarbeitung und -speicherung

- Große Mengen an Daten, z. B. von Aufklärungssystemen, Überwachungssystemen oder Kommunikationsnetzwerken, können besser und effizient verarbeitet, analysiert, ausgewertet und gespeichert werden. Hierfür können u. a. KI-Systeme genutzt werden.
- Cybersicherheit: Cloud-Computing bietet fortschrittliche und innovative Sicherheitsmaßnahmen zum besseren Schutz von sensiblen Informationen. Es können Angriffe besser erkannt und (automatisiert) Reaktionen eingeleitet werden, um Schäden oder Informationsabflüsse zu verhindern.
- Virtualisierung und Simulation: Simulations- und Trainingsumgebungen können über Cloud-Services angeboten und unabhängig vom Ort genutzt werden.
- Logistik und Supply-Chain-Management: Unterstützung bei der Verwaltung von Lieferketten und logistischer Prozesse, z. B. bei der Verfolgung von Ressourcen, Bestandsmanagement, Planung und Koordination von Nachschüben und Transporten

**Softwareentwicklungsplattform**

- Software-Factory
- Agile Softwareentwicklung mit modernen Entwicklertools
- CI / CD Pipeline
- DevSecOps

**Weitere Anwendungsfelder sind beliebig erweiterbar.**

## Herausforderungen

- Kontrolle der Daten- und Softwarehoheit (verschiedene Cloudlösungen, diverse Anbieter) – somit Standortprüfung im Zuge der digitalen Souveränität (Wahlfreiheit zur Einbindung nationaler und internationaler Partner, bzw. mit Portabilität auch Möglichkeit anbieterunabhängig agieren zu können, z. B. Wechsel von Dienstleistern ohne Herausforderung durch containerisierte, modulare Lösungen | Klärung Verschlüsselung und Zugriff auf die Daten | **operative Souveränität** Transparenz und Kontrolle über den Betrieb des Anbieters durch Datentransparenz| **Softwarehoheit**: Workload unabhängig von der Software des Anbieters ausführen | **juristische Souveränität**: deutsche Gerichtsbarkeit für Datenplattform und darin enthaltene Daten – somit Schutz vor Drittstaatentransfer)
- Betrieb im Krisenfall klären (im Ausland auch unter Einbeziehung des Auswärtigen Amtes | im Inland mit zivilen Betreibern, die ggf. dann auch Kombattanten angesehen werden | Involvierung anderer Ressorts auf BMI, AA und BMVg beschränken, da Strukturen legitime Angriffsziele sind und nicht alle Ressorts involvieren sollten)
- Anforderungen an Konnektivität zu Partnern im In- und Ausland, auch mit Blick zur Fähigkeit Verschlusssachen – nur für den Dienstgebrauch (VS-NfD) GEHEIM | NATO Mission Secret
- Interoperabilität durch offene Schnittstellen und Standards

- Verteilung von Userinnen und Usern über diverse und weit entfernte Strecken – Schnelle Bereitstellung von Cloud-Workload in abgelegene Gebiete
- Robustheit stationärer oder mobiler Lösungen (Container) auch bei der Verfügbarkeit von lokalem Support und Betrieb mit Servicepersonal, das die SIcherheit prüft
- Detektierbarkeit durch Abstrahlung weiter optimieren, um Services auch in robusten Szenarien der Landes- und Bündnisverteidigung nutzen zu können
- Stärkung von Aspekten der Informationssicherheit (BSI C5 | IT-Grundschutz | Anbindung an andere Netze des Bundes | auch mit Blick aufdurch Behörden kontrollierte Updates | externe Schlüsselverwaltung | Zugriffskontrolle und Transparenz | Identitäten-Management | Security Operation Center)Vereinbarkeit der regulatorischen Anforderungen im Inland (des Datenschutzes | Data Acts | Geheimschutzbestimmungen und weitere Regulatorik Inland[1] | Friedensbetrieb) vs. dem Grundsatz Wirkung vor Deckung (geringe Bedeutung des Datenschutzes in robusten Szenarien) – dabei Autarkie im Krisenfall auch ohne Softwareupdates vs. technologische und infrastrukturelle Rahmenbedingungen und Notwendigkeiten, die zur Umsetzung eines funktionierenden, betreibbaren und wirksamen Cloud-Computing-Betriebsmodell (Datenverarbeitung, Kommunikation, Zugriff) erforderlich sind
- physische Absicherung der beiden Rechenzentren-Standorte der Bundeswehr | Standorte müssen einerseits autark und andererseits vernetzbar (»Spinnennetz«) mit (mobilen) BW-Einheiten sein
- Bei der Migration in die Cloud sind »alte und neue Welt« eine Zeit lang parallel zu betreiben. Allgemeine Akzeptanz der »neuen Welt« mit klaren »Leitplanken« und standardisierten Vorgaben für die Transformation von alt nach neu
- Bewusstsein und Wissen nicht vorhanden: Was bedeutet Cloud für die IT-Infrastruktur/Plattform (technologisch), für den operativen Betrieb, für Kundschaft/Nutzende, für die IT-Sicherheit, für die Kommunikation, den Zugriff und die Daten? Wie verändert sich das Betriebsmodell und wie der Konsum? Was bedeutet Cloud-Service? Welche gibt es und wie werden sie erzeugt? Welche Rollen sind notwendig, die es in der klassischen IT gar nicht gibt? Wer muss sich wie verändern und ggf. Verantwortung annehmen? Wie verändern sich Organisationsstrukturen? Welche Auswirkungen hat das auf die Rüstungsindustrie?
- Zu klären: Wer ist Cloud-Anbieter (Provider) innerhalb der Bundeswehr? Wer ist eigentlich Teil der Kundschaft? Welche Nutzerinnen und Nutzer gibt es? Wer ist für was zuständig? Gibt es ein Shared-Responsibility-Modell? Wer legt die Prozesse fest? Wie entsteht ein neuer Cloud-Service (bzw. »eine Anwendung«)? Wer darf einen Service anfordern? Schnittstellen, Rollen und Prozesse? Wie definiert sich ein Cloud-Mandant (Organisation, Teilstreitkraft, Kommando, Mission, Sicherheitszone, Anwendung, Standort etc.)? Welche Anforderungen und Eigenschaften gelten für die Mandatin bzw. den Mandanten (z. B. virtuelle Trennung, physische Trennung, erweiterte Sicherheitsmechanismen, Verfügbarkeiten, Konnektivität etc.)? Wie kann ein Cloud-Service von Nutzerinnen und Nutzern verwendet werden?

1 ↗ 2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf (datenschutzkonferenz-online.de)

## Bewertung und Handlungsempfehlungen

- »Die eine Cloud« kann es innerhalb der Bundeswehr nicht geben. »Multicloud Bundeswehr« ist bei der Bundeswehr als die Digitalisierungsplattform und überspannendes Betriebsmodell zu verstehen, um Cloud-Services auf einer standardisierten Abstraktionsebene betreiben zu können. Es wird viele Cloud-Instanzen geben, welche durch einen sog. »Cloud-Broker« zusammengefasst bzw. gesteuert werden.
- Es ist eine auf das Militär ausgerichtete Ausbildungskampagne notwendig, um die Antworten auf die Nutzungsmöglichkeiten von Cloud-Computing innerhalb der Bundeswehr festzulegen, wo Cloud-Computing Nutzen generiert und welche Veränderungen in Prozessen, Zuständigkeiten und Technologien in der Organisation notwendig werden (holistisches Konzept). Die handelnden Akteure bei den Teilstreitkräften der Bundeswehr, dem BAAINBW, der BWI und den Industriepartnern müssen transparent über die Veränderungen und definierten Standards informiert werden.
- Die Cloud muss die Ebenen VS-NfD Geheim (deutsch) und NATO Mission Secret abdecken und weitere Schnittstellen/ Absprachen zu den Ressorts Auswärtiges Amt und Bundesministerium des Innern haben. Andere Ressorts sind nicht zu involvieren, um im Falle eines Konfliktes nicht als direkte Angriffsziele inkludiert zu gelten.
- Heute noch geltende Fragen wie zur »Digitalen Souveränität« oder »IT-Sicherheit« oder »Datenschutzaspekte« werden durch die Prioritätensetzung »Wirkung vor Deckung« ergänzt. Daher sind ggf. Lücken hinzunehmen und die Funktionsfähigkeit im Einsatzfall in den Fokus zu nehmen. Der IT-Sicherheit ist grundsätzlich ein hoher Stellenwert beizumessen, in der Edge kann ggf. davon abgewichen werden. In der Cloud gibt es separate Informationsräume unterschiedlicher Einstufung. Zwischen ihnen müssen sinnvolle Brücken geschlagen werden.
- Cloud-Computing birgt Risiken bei der Informationssicherheit und dem Datenschutz, liefert aber gleichzeitig fortschrittliche Fähigkeiten, um die Informationssicherheit auszubauen und zu optimieren. Beides muss unter Berücksichtigung der Mehrwertpotentiale durch Cloud-Computing (»Wirkung vor Deckung«) einer Risikoanalyse unterzogen, bewertet und entschieden werden.
- Das BSI bzw. der CISO Ressort BMVg muss sich klar positionieren, mit welchen Rahmenbedingungen und in welcher Ausprägung Cloud-Computing (Private, Hybrid, Multi, Public) für bestimmte Szenarien und Sicherheitsdomänen akzeptabel ist. Dabei sollte auch die Bewertung von IT-Sicherheitsorganen anderer NATO-Partner mit einfließen und für die Bewertung der aktuelle technologische Entwicklungsstand und der Marktstandard herangezogen werden. Darüber hinaus muss ein Informationsrückfluss an die Technologieanbieter etabliert werden, um möglichen Sicherheitsbedenken durch Anpassungen und Weiterentwicklungen in der Sicherheitsarchitektur der Cloud-Lösungen begegnen zu können.
- Allgemein muss das Tempo und die Reaktionsgeschwindigkeit von BSI und DeuMilSAA erhöht werden.
- Nach dem Vorbild anderer NATO-Partner, wie UK und USA, muss **unbedingt** das Ziel verbindlich vereinbart werden, der Sicherheitsarchitektur eines Cloud-Providers zu vertrauen und entsprechend zu zertifizieren. Das bedeutet nicht zwingend, dass klassifizierte Daten unterschiedlicher Sicherheitszonen (VS-NFD Geheim etc.) gemeinsam gehostet und von der gleichen Serverhardware prozessiert werden, sondern vielmehr, dass Netzwerk- und Management-Komponenten übergreifend verwendet werden dürfen

und dafür eine physische äquivalente Trennung durch Verschlüsselung umgesetzt ist. Dadurch werden erhebliche Kosteneinsparungen durch den Wegfall einer strikten physischen Trennung der Sicherheitszonen möglich. In privaten Clouds können zusätzlich Betriebsaufwände reduziert und Bereitstellungszeiten deutlich verkürzt. Darüber hinaus ist ein deutlich geringerer Platzbedarf bei verlegefähigen Einheiten notwendig, die unterschiedliche Sicherheitszonen abdecken müssen (z. B. Fregatte).

- Die BWI ist für die »pCloudBw« als Agent nach Beschluss federführend und daher nicht mehr nur für die »weiße IT« zuständig. Vorhandene und neue Lösungen müssen jedoch mit Partnern auf Augenhöhe adaptiert werden.
- Es gibt nicht den einen Weg in die Cloud. Daher sind feststehende Projektverantwortliche zu identifizieren, die in Interaktion mit Partnern und Bedarfsträgern im engen Austausch agieren. Dabei ist eine frühzeitige Betrachtung von Architektur und Sicherheitsvorgaben zu beachten.
- Grundsätzlich muss ein technologieoffener Ansatz angedacht werden.
- Es muss das Zielbild angestrebt werden, eine einheitliche Interoperabilitätsplattform zu erzeugen, die über Cloud-Infrastrukturen unterschiedlicher Hersteller, Cloud Provider oder Hyperscaler geliefert werden kann
- Jeder Use Case ist einzeln zu betrachten und daraufhin Rahmenbedingungen zu setzen.
- Ein reines Lift & Shift (Verschiebung von Daten und Anwendungen in die Cloud, ohne Veränderungen am Design, Funktionsweisen, Code der Applikation etc.) ist nicht zielführend.
- Die Eigenentwicklung und Zulieferung alle verwendeten Anwendungen (COI, COTS, MOTS) müssen festgelegten Standards folgen. Damit Anwendungen Cloud-agnostisch betrieben werden können, dürfen Sie keine Abhängigkeiten zu infrastrukturnahen Komponenten oder Cloud-spezifischen Diensten haben. In der Fachsprache werden Anwendungen, die diese Eigenschaften erfüllen, als Cloud-native Applications (CNA) bezeichnet. Diese Anwendungen können in jeder Cloud in Betrieb genommen werden, wo eine Betriebsplattform mit den notwendigen Fähigkeiten existiert, und bestehen in der Regel aus Open Source Software-Komponenten. Diese Standards müssen definiert und die Einhaltung bei der Beschaffung von Anwendungen eingefordert werden.
- Es muss eine Transformation aller Anwendungen in Richtung Cloud-native Applications, möglichst unter Verwendung von Open Source Software angestrebt werden
- Die Cloud kann keine Interoperabilität zwischen verschiedenen Anwendungen erzeugen. Die Standards für den Daten- und Informationsaustausch zwischen verschiedenen Anwendungen und Waffensystemen innerhalb der Bundeswehr und zwischen den Bündnispartner müssen durch einheitliche Datenformate, Protokolle und Schnittstellen festgelegt und umgesetzt werden. Diese Abstraktionsebene ist unabhängig von einem Cloud-Betriebsmodell. Dies betrifft insbesondere Programme, wie Multi-Domain-Combat-Cloud.
- containerisierte Anwendungen (Standard Kubernetes) für die Interoperabilität in der Cloud
- Bei der Migration sind zusätzliche Ressourcen bei der Betriebsunterstützung nötig.
- Mit der Cloud entstehen neue Aufgabenfelder und Profile, bzw. erfordert dies neue Skills und alte Modelle werden verändert. Hier ist der Change auf Ebene der Mitarbeitenden zu begleiten und aktiv zu gestalten.

- Mobile Cloudlösungen umfassen: eine transportable Lösung mit geringem Gewicht »rugged device« für den Einsatz zu Land, Wasser, Luft und extremen Bedingungen, lauffähig mit und ohne Cloud-Connect
- Bündnistauglichkeit umfasst: taktische Integration in D-LBO, als technologische Edge-Komponente | Umsetzung der NATO-Vorgaben in einen sicheren »Building Block«| Unterstützung bei der Umsetzung der Public Cloud einschließlich Sovereign Cloud
- Prüfung, ob kommunale IT-Dienstleister einzubinden sind, bzw. eingebunden werden können