04/2026

sopra steria

a Sopra Steria company

RESILIENTE WELTRAUMARCHITEKTUR: VERNETZT. VERTEILT. VERTEIDIGUNGSFÄHIG.

Die Raumfahrt steht vor einem grundlegenden Paradigmenwechsel. Steuerung, Entscheidungslogik und Datenverarbeitung verlagern sich zunehmend vom Boden in den Orbit. Satelliten entwickeln sich von passiven Sensorplattformen zu autonomen, vernetzten Akteuren, die Informatioxnen vorverarbeiten, priorisieren und in Teilen selbstständig handeln können. Gleichzeitig wird der Weltraum zu einem militärischen Operationsraum, in dem andere Raumfahrtnationen Nahkampfmanöver erproben und europäische Satelliten abhören. Dafür braucht Deutschland eine sichere, multiorbitale, softwaredefinierte Gesamtarchitektur mit resilientem Betriebsmodell und sicherem IT-Backbone.

TECHNOLOGISCHER UMBRUCH – VOM BODENZENTRIERTEN ZUM ORBITZENTRIERTEN SYSTEM

Die Raumfahrt befindet sich an einem technologischen Wendepunkt, der auf den tiefgreifenden Umbrüchen der vergangenen Dekade aufbaut – beschleunigt insbesondere durch die Kommerzialisierung der Raumfahrt durch Akteure wie das US-amerikanische Unternehmen SpaceX. Sinkende Startkosten, Miniaturisierung und neue industrielle Akteure haben die Eintrittshürden gesenkt und die Skalierung weltraumgestützter Systeme verändert. Gegenwärtig kommt ein weiterer Paradigmenwechsel hinzu: die Abkehr vom bodenzentrierten Raumfahrtmodell. Traditionell lag der Schwerpunkt auf leistungsfähigen Bodenstationen: Missionslogik, Steuerung und Datenverarbeitung wurden überwiegend terrestrisch realisiert, während Satelliten vor allem als ferne Datensammler fungierten. Diese Architektur machte das Bodensegment zum kritischen Knotenpunkt – technisch leistungsfähig, aber zugleich hochgradig verwundbar.

Weltraumgestütztes Edge Computing ist ein klarer Ausdruck des Paradigmenwechsels: Statt Daten ausschließlich im Orbit zu sammeln und zur Verarbeitung an Bodenstationen zu senden, erfolgt die Datenverarbeitung zunehmend direkt an Bord des Satelliten. Damit müssen Sensordaten nicht mehr vollständig zum Boden übertragen werden. On Board KI filtert, klassifiziert und priorisiert Daten (z. B. Wolkenmaskierung, Objekt-/Ereignisdetektion) und sendet nur die relevanten – das kann Reaktionszeiten verkürzen und Downlink-Ressourcen entlasten.

EDGE COMPUTING UND KI

Beim Einsatz von KI im Weltraum ist der erste Schritt immer derselbe: den Anwendungsfall sauber zu konzipieren. Allzu oft werden direkt Schlagworte genannt. Dabei verliert man aus dem Blick, welches Problem eigentlich gelöst werden soll. Eines der gängigsten Argumente für Edge-KI im Orbit lautet, dass sie Latenz reduziert und Bandbreite spart: Satelliten können Daten bereits im All vorverarbeiten und nur diejenigen, die wirklich relevant sind, zur Erde zurücksenden. In vielen Szenarien trifft das zu.

Der entscheidende Punkt ist jedoch: Der Engpass ist zunehmend nicht die Latenz, sondern die Bandbreite. Denn die zunehmende Verlagerung von KI-Systemen in den Orbit trifft auf eine weitere technologische Entwicklung: riesige Satellitenkonstellationen. Beide, KI im Orbit sowie Megakonstellationen, bedingen einander und sind entscheidend für das Thema Datenverarbeitung. Denn Hunderte oder Tausende von Satelliten kommunizieren nicht nur mit der Erde, sondern sind untereinander vernetzt und kommunizieren über optische Inter-Satellite-Links miteinander. In so verbundenen Megakonstellationen bewegen sich Daten innerhalb einer Konstellation schnell zum jeweils bestpositionierten Downlink-Knoten. Sie können also mit Lichtgeschwindigkeit bewegt werden. Am Boden werden auch weiterhin intelligente Auswertesysteme eingesetzt. Gleichzeitig wächst der strukturelle Druck auf Downlink Kapazitäten, Kontaktfenster und das knappe Radio Frequency (RF) Spektrum – und zwar nicht irgendwann, sondern bereits im aktuellen Betrieb.

Das eigentliche Engpassproblem wird in Zukunft daher selten die reine Latenz sein – und zunehmend auch nicht die Rechenleistung an Bord. Der strukturelle Flaschenhals ist die Bandbreite: Downlink-Kapazitäten und das knappe RF Spektrum.

Und diese Knappheit ist kein zukünftiges Risiko, sondern bereits heute eine der entscheidenden operativen Einschränkungen.

In der Praxis zeigt sich dabei ein wiederkehrendes Muster: Satelliten generieren weit mehr Daten, als wir herunterladen können; Kontaktfenster sind kurz und selten; wachsende Konstellationen konkurrieren um begrenztes Spektrum; und große Mengen an Erdbeobachtungsdaten sind operativ wenig wertvoll, verstopfen aber dennoch die Pipeline. Für taktische Missionen kommt hinzu: Es ist schlichtweg keine Option, erst Stunden später am Boden auf Auswertung zu warten.

Damit wird KI im Orbit von der „Optimierung" zur betriebsnotwendigen Funktion: Triage, Komprimierung und intelligente Auswahl sind nötig, weil Satelliten mehr Daten erzeugen, als zuverlässig übertragen werden können – und weil taktische Nutzung keine stundenlange Verzögerung am Boden toleriert. Edge-KI ist damit nicht nur ein Feature, sondern auch ein definierender Teil der neuen Architektur unserer Weltraumsysteme.

Internationale Entwicklungen unterstreichen diese Richtung. Medienberichte über den Aufbau einer chinesischen „Three Body Computing Constellation" im Frühjahr 2025, bei der KI-Inferenz über ein hochgeschwindigkeitsfähiges Satellitennetzwerk im Orbit erfolgt, verdeutlichen, dass Rechenleistung im All zunehmend als strategische Ressource verstanden wird. Der Orbit wird damit nicht nur zum Sensorraum, sondern auch zum verteilten Rechen- und Entscheidungsraum.

SOFTWARE-DEFINED SPACE

Parallel dazu verstärkt sich ein übergreifender Technologietrend: die Softwaredefinition von Systemen. In anderen Dimensionen der Bundeswehr, allen voran Land, wird diese Entwicklung unter dem Begriff Software Defined Defence (SDD) diskutiert – also der konsequenten Nutzung von Software, Updates und datengestützten Verbesserungen, um militärische Fähigkeiten schneller, flexibler und kontinuierlich weiterzuentwickeln.

In der Raumfahrt deutet sich mit Software Defined Satellites (SDS) und Software Defined Radio (SDR) eine vergleichbare Entwicklung an. Software rückt von einer unterstützenden Rolle zu einem zentralen Hebel für Leistungsfähigkeit, Anpassungsfähigkeit und Überlebensfähigkeit im Betrieb. Wenn Softwareupdates in der Raumfahrt früher als Risiko galten und möglichst vermieden wurden, werden sie künftig zur Voraussetzung militärischer Handlungsfähigkeit.

Diese Entwicklung ist nicht rein technisch. Sie verändert Innovationszyklen, Betriebsmodelle und sicherheitspolitische Abhängigkeiten. Fähigkeiten entstehen nicht mehr primär durch neue Hardwaregenerationen, sondern durch kontinuierliche Weiterentwicklung im Betrieb. Die unterschiedlich schnellen Innovationszyklen von Hard- und Software gilt es zu akkommodieren. Gleichzeitig steigt der Anspruch an Sicherheit, Integrität und Nachweisbarkeit von Software und Daten – insbesondere in hochvernetzten, verteilten Systemen im All.

DER WELTRAUM ALS WARFIGHTING DOMAIN

Hand in Hand und einander bedingend geht mit der technologischen Aufwertung des Orbits eine sicherheitspolitische Neubewertung einher. Weltraumsysteme werden nicht länger nur als unterstützende Infrastruktur betrachtet, sondern zunehmend als eigenständige militärische Wirkdimension. Der Weltraum ist zu einer Warfighting Domain geworden – einem militärischen Operationsraum, in dem staatliche Akteure gezielt Fähigkeiten aufbauen, erproben und einsetzen.

Die Verwundbarkeit weltraumgestützter (ziviler) Infrastrukturen wurde bereits vor einigen Jahren sichtbar. Zu Beginn des Ukrainekrieges machte ein Cyberangriff auf das KA-SAT-Netzwerk von Viasat deutlich, wie anfällig bodenzentrierte Architekturen sein können: Durch die Manipulation der Bodeninfrastruktur wurden innerhalb weniger Stunden tausende Modems unbrauchbar gemacht, militärische wie zivile Kommunikation beeinträchtigt und die Fernsteuerbarkeit zahlreicher Windenergieanlagen in Deutschland eingeschränkt.

Weniger öffentlich wahrgenommen, aber strategisch ebenso relevant, ist die zunehmende Aktivität gegnerischer Akteure direkt im Orbit. Russische Satelliten wie Luch 1 und Luch 2 sind europäischen Sicherheitsbehörden aufgefallen und stehen im Verdacht, Kommunikationsverbindungen anderer Satelliten abgefangen zu haben. Solche Aktivitäten verdeutlichen, dass hybride Operationen längst nicht mehr an der Atmosphäre enden, sondern gezielt in den Weltraum verlagert werden.

Mit zeitlicher Verzögerung haben der Ukrainekrieg und die deutsche Zeitenwende auch in der militärischen Raumfahrt zu einem Umbruch geführt. Wissenschaftliche Exploration tritt hinter Abschreckung, Resilienz und einem beispiellosen militärischen Fähigkeitsaufbau zurück.

FÜR EINE RESILIENTE DEUTSCHE WELTRAUMARCHITEKTUR

Die Bundesregierung spricht in ihrer Weltraumsicherheitsstrategie von einer Weltraumsicherheitsarchitektur, die sich durch drei Beschreibungen auszeichnet: wehrhaft, resilient, kooperativ. Eine solche hochanspruchsvolle Leistung wird Deutschland nur durch die verstärkte Zusammenarbeit mit der Industrie realisieren können.

Gleichzeitig muss dem eingangs beschriebenen Paradigmenwechsel zum Edge Computing Rechnung getragen werden. Wenn Compute, Missionslogik und Entscheidung zunehmend in den Orbit wandern, verschiebt sich auch die Architektur militärischer Raumfahrt: weg von wenigen zentralen Bodenstationen und Bodensegmenten, hin zu einem verteilten, softwaregestützten System of Systems (SoS) mit höherer Resilienz.

ZIELARCHITEKTUR RESILIENTE WELTRAUMARCHITEKTUR
(Technologie – Betrieb – Sicherheit – Daten – Rekonstitution)

STRATEGISCHE / POLITISCHE EBENE
Auftrag • Abschreckung • ROE • Nationale Sicherheit • NATO/EU-Interoperabilität

↓

SPACE DOMAIN AWARENESS / WELTRAUMLAGE
Space Surveillance • Missile Warning • Objektkatalog • Anomalieerkennung
Attribution • Threat Intelligence • Lagebild für Schutz / Abwehr / Rekonstitution

↓

ORBIT-SEGMENT
GEO/LEO/MEO Satelliten • ISR • SATCOM • Missile Tracking • PNT • On-board Compute
Edge AI • optische Inter-Satellite-Links • gehostete Nutzlasten • verteilte Knoten

↓

LINK-SEGMENT
RF • Laser • Crosslinks • Gateway
Routing • alternative Pfade
Jamming-/Spoofing-Schutz

GROUND-SEGMENT
Bodenstationen • Missionsbetrieb
Cloud / Rechenzentren • Data Layer
SOC / NOC / DevSecOps / C2

↓

C2 / MISSION- UND BETRIEBSMODELL
Sensor Fusion • Entscheidungsunterstützung • AI Battle Management • Workflow
Missionsplanung • Priorisierung • Incident Handling • degradierter Betrieb

↓

SICHERER IT-BACKBONE
Zero Trust • Identitäten • Kryptographie / PQC • Telemetrie • Monitoring
Security by Design • SOAR/SIEM • Update- und Patch-Pipelines • Nachweisbarkeit
Integrität von Daten, Software, Modellen und Konfigurationen

↓

SOVEREIGN DATA LAYER
Datenklassifikation • Data Governance • Provenance • Data Contracts
Metadaten • Datenräume • Speicher-/Compute-Placement • Sharing-Regeln
Interoperabilität zwischen Konstellationen, Partnern und Führungs-/Waffensystemen

↓

RESILIENZ / REKONSTITUTION / WIEDERAUFBAU
Disaggregation • Distribution • Redundanz • Ausweichpfade • Graceful Degradation
Ersatzsatelliten • Responsive Launch • On-Orbit Servicing • Repair / Replenishment
Wiederanlauf von Diensten • Daten-/Software-Recovery • Rekalibrierung

↓

INDUSTRIE- UND BESCHAFFUNGSÖKOSYSTEM
Satellitenbauer • IT-/Cyber-Unternehmen • Start-ups • Forschung • Bundeswehr
Test-/Demo-Missionen • DevSecOps • Supply Chain Assurance
Serienfähigkeit • Betrieb • Nachrüstung • kontinuierliche Fähigkeitsentwicklung

↓

QUERSCHNITTLICHE LEITPLANKEN ÜBER ALLE EBENEN
Interoperabilität / offene Schnittstellen
Digitale Souveränität / Kontrolle über Schlüssel, Daten, Modelle und Updates
Supply-Chain-Sicherheit / Hardware Trust / Herkunftsnachweise
- Multi-Orbit / Multi-Path / Multi-Partner
Schutz, Aufklärung, Abwehr, Rekonstitution und kontinuierliche Weiterentwicklung

Im Folgenden wird beschrieben, was aus industrieller Sicht notwendig sein wird, um eine solche resiliente, wehrhafte Weltraumarchitektur aufzubauen, die aktuelle technologische Trends adressiert.

ES ERGEBEN SICH FOLGENDE ZENTRALE HANDLUNGSFELDER:

- Vernetzung im Orbit
- Space Domain Awareness
- Resilienz-steigernde Aspekte
- IT- und Betriebsmodell, das verteilte Systeme Ende zu Ende absichert
- souveränes Daten-management
- Fähigkeit, Technologien neu und anders zu beschaffen

Positioning, Navigation and Timing (PNT) ist eine zentrale Voraussetzung für Koordination, Synchronisation und Kommunikation in weltraumgestützten Systemen, wird jedoch in diesem Papier bewusst nicht vertieft behandelt. Der Fokus dieses Beitrags liegt auf Architektur , Betriebs- und Sicherheitsfragen verteilter, softwaredefinierter Weltraumsysteme; PNT Aspekte werden als grundlegende Fähigkeiten vorausgesetzt.

ERLÄUTERUNGEN ABKÜRZUNGEN:

ROE – Rules of Engagement
ISR – Intelligence, Surveillance & Reconnaissance
PNT – Positioning, Navigation & Timing
RF – Radio Frequency
SOC – Security Operations Center
NOC – Network Operations Center
C2 – Command & Control
PQC – Post-Quantum Computing

1. VERNETZUNG IM ORBIT

Die Weltraumsicherheitsstrategie verspricht eine „vernetzte, multiorbitale Gesamtarchitektur". Diese setzt voraus, dass künftige Konstellationen nicht als Insellösungen betrieben werden, sondern als integriertes Netzwerk über Orbits hinweg funktionieren – mit standardisierten Schnittstellen, verteiltem Datentransport und der Fähigkeit, Informationen dynamisch über den jeweils günstigsten Pfad zum Boden zu routen. Außerdem müssen Konstellationen, die unterschiedlichen Zwecken dienen (etwa Kommunikation und Reconnaissance), miteinander arbeiten können.

Für diese Art von orbitaler Vernetzung sind optische Inter-Satellite-Links (Laser) der technologische Schlüssel: Sie ermöglichen sehr hohe Datenraten und entlasten das knappe RF-Spektrum. Im Vergleich zu klassischen Funkstrecken bieten sie eine deutlich höhere Robustheit gegenüber Störung und Abhören. Parallel dazu ist ein klarer Trend hin zu verstärktem Einsatz optischer Bodenstationen zu beobachten.

Genau diese Logik wird in Europa bereits praktisch umgesetzt – etwa durch das European Data Relay System (EDRS),[1] das als laserbasiertes Relaisnetz Daten aus dem Low Earth Orbit (LEO) über geostationäre Knoten mit optischen Links zur Erde überträgt und die erste kommerzielle Anwendung optischer Satellitenkommunikation im Weltraum bildet.[2] Gleichzeitig zeigt EDRS auch: Vernetzung endet nicht im Orbit, sondern erfordert ein leistungsfähiges Bodensegment aus Kontrollzentren und einem Netz von Bodenstationen, das die optischen Links zuverlässig „abholt".

Laserkommunikation ist technisch anspruchsvoll – insbesondere durch die Atmosphärenpassage und die notwendige präzise Nachführung –, weshalb Forschungs- und Demonstrationsinfrastrukturen wie die Optische Bodenstation Oberpfaffenhofen (OGSOP) mit Tracking-Funktion, adaptiver Optik und Experimenten bis hin zur Quantenschlüsselverteilung eine zentrale Rolle für die Reife und Skalierung solcher Architekturen spielen.

Der letzte Aspekt – aus dem Bereich der Forschung – wird in Zukunft eine wichtige Rolle spielen: Optische Verbindungen gelten nicht nur als Backbone für Daten, sondern auch als Träger für zukunftsfähige Kryptographieansätze und bilden damit einen Baustein für spezielle hochsichere Kommunikationspfade. Die ESA entwickelt mit QKDSat beispielsweise einen weltraumgestützten Demonstrator für Quantum Key Distribution zur sicheren Schlüsselverteilung.[3]

In Summe entsteht so eine Architektur, die zugleich skalierbar und resilient ist: Wenn Konstellationen wachsen, kann der Ausfall einzelner Satelliten den Gesamtdienst nur begrenzt beeinträchtigen – ein Kernprinzip verteilter Netze.

[1] ESA - Data-relay satellite ready for service
[2] EDRS - European Data Relay System
[3] ESA - QKDSat: Secure communication via quantum cryptography

2. SPACE DOMAIN AWARENESS

Space Domain Awareness (SDA) ist eine Grundvoraussetzung für Schutz, Wirkung und Resilienz. Der erste Schritt zum Schutz weltraumgestützter Infrastrukturen besteht darin, sicherheitsrelevante Ereignisse und Bedrohungen im Weltraum überhaupt erkennen, einordnen und – soweit möglich – attribuieren zu können. In einer verteilten, multiorbitalen Weltraumarchitektur ist SDA deshalb keine nachgelagerte Unterstützungsfunktion, sondern eine operative Kernfähigkeit. Wer den Weltraum als eigenständigen Operationsraum begreift, muss auch in der Lage sein, diesen Raum kontinuierlich zu beobachten, Veränderungen frühzeitig zu erkennen und daraus belastbare Handlungsoptionen abzuleiten.

SDA umfasst dabei mehr als klassisches Space Surveillance and Tracking. Erforderlich ist ein integriertes Lagebild aus zivilen, militärischen und kommerziellen Sensoren, das nicht nur Objekte katalogisiert, sondern auch Verhalten, Annäherungen, Anomalien, potenzielle Störungen und Angriffsmuster bewertet. Dazu gehören optische und radarbasierte Weltraumüberwachung, weltraumgestützte Infrarotsensorik zur Raketenfrühwarnung, Telemetriedaten aus eigenen Konstellationen, Informationen aus dem elektromagnetischen Spektrum sowie die Zusammenführung externer Partnerdaten. Ziel ist nicht nur die geometrische Verfolgung von Objekten, sondern ein belastbares Verständnis von Aktivität, Absicht und Bedrohungsrelevanz.

Für eine resiliente deutsche Weltraumarchitektur erfüllt SDA vier Funktionen.

1. Frühwarnung: Raketenstarts, ungewöhnliche Annäherungen, Jamming-Muster oder Veränderungen im Verhalten gegnerischer Systeme müssen möglichst früh erkannt werden.
2. Entscheidungsfähigkeit: Nur wenn Beobachtungen zu einem konsistenten Lagebild zusammengeführt werden, können politische und militärische Akteure angemessen reagieren.
3. Schutz- und Rekonstitutionsfähigkeit: Ausweichmanöver, Lastverlagerung, Priorisierung von Diensten oder die Aktivierung von Ersatzressourcen setzen voraus, dass eine Bedrohung nicht nur technisch erkannt, sondern operativ eingeordnet wird.
4. Wirkfähigkeit: Wer gegnerische Weltraumnutzung einschränken oder gegnerisches Verhalten abschrecken will, benötigt eine robuste Lagegrundlage.

Mit dem Übergang zu softwaredefinierten und stärker autonomen Architekturen gewinnt SDA zusätzlich an Bedeutung. Ein Teil der Lageerstellung und Anomalieerkennung wird künftig nicht mehr ausschließlich am Boden erfolgen können, sondern muss – zumindest in Vorstufen – in den Orbit verlagert werden. On-Board-Wahrnehmung, Sensorfusion und ereignisbasierte Priorisierung verkürzen Reaktionszeiten und verringern die Abhängigkeit von Bodenstationen. Gleichzeitig steigen die Anforderungen an die Vertrauenswürdigkeit von Sensordaten, an die Validierung von KI-gestützten Erkennungsverfahren und an die sichere Übertragung der gewonnenen Erkenntnisse.

SDA ist damit der Ausgangspunkt einer handlungsfähigen Weltraumarchitektur. Ohne Weltraumlage bleiben Resilienz, Schutz, Wirkung, Rekonstitution und politische Entscheidungsfähigkeit reaktiv und fragmentiert. Mit ihr wird der Orbit vom bloßen technischen Trägerraum zu einem beobachtbaren, bewertbaren und gestaltbaren Operationsraum.

3. RESILIENZ, REKONSTITUTION UND WIEDERAUFBAU

Weltraumgestützte Dienste sind für Führung, Aufklärung, Kommunikation und Wirkung auf der Erde unverzichtbar, zugleich aber dauerhaft gefährdet. In einem sicherheitspolitisch umkämpften Umfeld reicht es daher nicht aus, Systeme nur gegen Ausfälle oder Angriffe zu härten. Entscheidend ist vielmehr, ob eine Architektur auch unter Störung, Teilverlust oder Angriff weiterhin handlungsfähig bleibt, kritische Funktionen priorisieren kann und ihre Fähigkeiten in vertretbarer Zeit wiederherstellt. Resilienz ist deshalb nicht nur Widerstandsfähigkeit, sondern die Kombination aus Weiterbetrieb unter Belastung, schneller Rekonstitution und planbarem Wiederaufbau. Folgende Fähigkeitskomponenten sollten in Weltraumsystemen abgebildet werden:

1. Schutz (Protection) umfasst passive Maßnahmen, die Satellitensysteme intrinsisch robuster machen, etwa physische oder elektromagnetische Härtung. Dazu zählen der Schutz des Verbindungssegments gegen Störsender (Jamming) und andere Interferenzen sowie softwarebasierte Maßnahmen wie Verschlüsselung. Ergänzend können integrierte Fähigkeiten zur Erkennung und Bewertung möglicher Angriffe, darunter auch Cyberangriffe, sowie verbesserte Manövrierfähigkeit für aktive Ausweichbewegungen schutzorientiert wirken. Schutz ist jedoch nur die erste Linie. Er vermindert die Eintrittswahrscheinlichkeit und die unmittelbare Wirkung eines Angriffs, ersetzt aber nicht die Fähigkeit, nach Störung oder Verlust wieder in einen belastbaren Betriebszustand zurückzukehren.

2. Disaggregation und Distribution sind komplementäre Architekturprinzipien: Systeme werden entweder funktional in getrennte Teilsysteme aufgeteilt (Disaggregation) oder missionsgleich über mehrere Einheiten verteilt (Distribution), sodass der Ausfall einzelner Plattformen die Gesamtfähigkeit nicht sofort lahmlegt. Disaggregierte Architekturen erhöhen nicht nur die Überlebensfähigkeit, sondern erleichtern auch Rekonstitution und Modernisierung, weil einzelne Subsysteme gezielt ersetzt, ergänzt oder neu ausgebracht werden können. Im Hinblick auf Resilienz ist dies der Übergang von der Logik „eine Plattform – ein kritischer Ausfallpunkt" hin zu einem Netz robuster, austauschbarer und teilersetzbarer Funktionsknoten.

3. Resilienz muss um Graceful Degradation und Betrieb in degradierten Modi erweitert werden. Eine moderne Weltraumarchitektur sollte nicht zwischen „voll funktionsfähig" und „ausgefallen" unterscheiden, sondern abgestufte Betriebszustände kennen. Unter Störung müssen Dienste priorisiert, Datenflüsse neu geroutet, nichtkritische Funktionen temporär abgeschaltet und kritische Missionen auf alternative Plattformen oder Segmente verlagert werden können. Gerade verteilte Konstellationen mit Inter-Satellite-Links und softwaredefinierten Funktionen bieten hier die Möglichkeit, eingeschränkten Betrieb aufrechtzuerhalten, anstatt das Gesamtsystem zu verlieren.

4. Eine resiliente Architektur braucht eine explizite Rekonstitutionslogik. Dazu gehört die Fähigkeit, verlorene oder degradierte Funktionen durch Ersatzsatelliten, gehostete Nutzlasten, zusätzliche Startfenster, alternative kommerzielle Dienste (etwa Erdbeobachtungsdaten privater Anbieter, u. a. innovativer Start-ups) oder Umverteilung innerhalb bestehender Konstellationen wiederherzustellen. Rekonstitution ist damit nicht nur ein technischer, sondern auch ein industrieller und logistischer Begriff: Ersatz muss beschaffbar, startbar, integrierbar und betrieblich aufnehmbar sein. Eine Resilienzstrategie ohne Rekonstitution bleibt unvollständig, weil sie den Verlust zwar verzögert, aber nicht systematisch beantwortet.

5. Dazu gehört der Wiederaufbau von Daten- und Betriebsfähigkeit. Nach einem Angriff oder Systemfehler reicht es nicht, Hardware oder Verbindungen wieder verfügbar zu machen. Ebenso wichtig ist die Wiederherstellung verlässlicher Datenbestände, Konfigurationen, Schlüsselmaterialien, Softwarestände und Modelle. Eine Architektur muss daher auch auf der Ebene von Daten, Identitäten, Konfigurationen und Missionsparametern recoveryfähig sein. Andernfalls entstehen technisch verfügbare, aber operativ nicht vertrauenswürdige Systeme.

6. Resilienz ist ohne zivil-militärische Diversifikation nur begrenzt erreichbar. Die Nutzung ziviler und kommerzieller Dienste, etwa für Erdbeobachtung, Kommunikation oder ergänzende Datenquellen, kann die Robustheit der Gesamtarchitektur erhöhen. Allerdings muss diese Diversifikation bewusst gesteuert werden: Dual Use erhöht Reichweite und Redundanz, schafft aber zugleich neue Abhängigkeiten und Schutzanforderungen. Resilienzgewinn entsteht daher nicht automatisch durch mehr Anbieter, sondern durch ein gezielt gestaltetes Portfolio aus eigenen, staatlich kontrollierten und kontrolliert eingebundenen kommerziellen Fähigkeiten.

Militärische Systeme sind meist stärker gehärtet und bedienen einen kleineren Nutzerkreis; dennoch ist plausibel, dass auch zivile Betreiber ihre Schutzmaßnahmen ausbauen, da ihre Systeme im Krisen- oder Konfliktfall ebenfalls Ziele sein können. Vor diesem Hintergrund sollte über folgende Möglichkeiten zumindest ernsthaft nachgedacht werden:

- Laserbasierte Satellitenkommunikation könnte auch für kommerzielle (kleinere) Konstellationen, z. B. im Bereich der Erdbeobachtung, eingesetzt werden. Der schmale, gerichtete Strahl ist schwer abzufangen oder zu stören, entlastet das überlastete Frequenzspektrum und eignet sich besonders für leistungsfähige Inter-Satelliten-Netzwerke in modernen Konstellationen.
- Was spricht dagegen, auch zivile Satelliten in die Früherkennung von Raketenstarts einzubinden? Weltraumgestützte Infrarotsensoren können die Wärmesignatur von Raketenantrieben bzw. hypersonischen Flugkörpern direkt beim Start und in der frühen Flugphase detektieren. Beobachtung „von oben" ist nicht durch Radarhorizont, Geländeabschattung oder Wettereffekte eingeschränkt und liefert potenziell frühere Warnungen als bodengebundene Sensoren – mit dem Vorteil zusätzlicher Vorwarnzeit zur Aktivierung von Abwehrsystemen sowie zur Unterstützung politischer und militärischer Entscheidungsprozesse.
- Mit dem Ende des bodenzentrierten Raumfahrtparadigmas verlagern sich Steuerung, Entscheidungslogik und Verarbeitung in den Orbit: Satelliten werden von reinen Sensorplattformen zu autonomeren Akteuren. Voraussetzung dafür ist die Fähigkeit der Satelliten, ihre unmittelbare Umgebung mithilfe geeigneter Sensoren selbstständig zu beobachten, um Bedrohungen oder Annäherungen frühzeitig zu erkennen. Erst diese On Board Wahrnehmung ermöglicht KI-gestützte autonome Entscheidungen, z. B. Ausweichmanöver in Echtzeit, ohne auf zeitverzögerte und potenziell angreifbare Bodenstationen angewiesen zu sein.

Resilienz in der militärischen Raumfahrt bedeutet damit mehr als Redundanz. Sie umfasst Schutz, verteilte Architektur, degradierte Betriebsfähigkeit, Rekonstitution verlorener Funktionen und den Wiederaufbau vertrauenswürdiger Betriebs- und Datenzustände. Erst das Zusammenspiel dieser Elemente macht aus einer technologisch modernen Konstellation ein tatsächlich wehrhaftes System.

4. SICHERER IT-BACKBONE

Die eingangs beschriebene Datenverarbeitung an Bord von Satelliten ist nicht nur eine technische, sondern auch eine strategische Frage: Sie markiert einen Paradigmenwechsel von zentraler Kontrolle über Bodenstationen hin zu verteilter Intelligenz im All. Entsprechend muss der IT-Backbone der gesamten Infrastruktur neu gedacht werden. Wenn Compute und Missionslogik in den Orbit wandern, muss auch das Betriebs- und Sicherheitsmodell teilweise mitwandern.

Cybersicherheit war kein treibendes Thema, als die Kommerzialisierung des Weltraums begann; die Raumfahrttechnik wurde von Systemsicherheitsforschern weitgehend übersehen. Entsprechend schlecht sind viele Satellitenoperateure aufgestellt, was die Härtung und Sicherung ihrer Systeme betrifft. So zeigten Forscher bereits mehrmals Vulnerabilitäten in Satelliten auf oder gewannen sogar Zugriff auf Satelliten.[4] Nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) sind für Akteure, die selbst nicht über weltraumfahrende Fähigkeiten verfügen, Cyberangriffe sowie Operationen im elektromagnetischen Spektrum die einzig realistischen Angriffsvektoren, um Weltraumsysteme zu stören, auszuspähen oder zu beeinträchtigen. Daher sind Weltraumsysteme und ihre kritischen Infrastrukturen mittlerweile stärker in den Fokus der Cyber-Sicherheitsforschung gerückt.

Mit einer zunehmenden Anzahl von Satelliten im All vergrößert sich per definitionem die Angriffsfläche unserer Gesellschaften im Orbit. Gleichzeitig stoßen klassische Cybersicherheitsmodelle (Perimeter, Zugriffskontrolle, Verantwortlichkeit) an ihre Grenzen, sobald Verarbeitungs- und Entscheidungsfunktionen in verteilte, hochdynamische und nur eingeschränkt kontrollierbare Weltrauminfrastrukturen wandern.

Das bedeutet: Was im IT-Betrieb am Boden seit Jahren als Security Operations Center (SOC) etabliert ist, muss für Konstellationen neu gedacht und in Teilen in den Orbit verlagert werden – inklusive Monitoring, Incident Handling und Recovery. So genannte SOCs gibt es seit den frühen 2000er-Jahren, als Unternehmen begannen, zentrale Einheiten für die Überwachung und Analyse von IT-Sicherheitsereignissen aufzubauen. Ursprünglich waren SOCs stark regelbasiert und arbeiteten mit klassischen SIEM-Systemen (Security Information and Event Management), die Logdaten sammelten und auf bekannte Muster prüften.

Moderne SOCs hingegen entwickeln sich zu so genannten NextGen-SOCs, die KI-gestützte Anomalieerkennung, Automatisierung (Security Orchestration, Automation and Response – SOAR) sowie Cyber Threat Intelligence (CTI) integrieren. Dabei liegen die Forschungsschwerpunkte auf Automatisierung, Adaptive Security und erklärbarer KI, um die Reaktionszeiten zu verkürzen und die Effizienz zu steigern. Terrestrische SOCs haben sich weltweit bewiesen und bewährt. Werden sie weiterentwickelt und an den Weltraum angepasst, können sie auch hier unterstützen.

Neben dem SOC-Gedanken spielt auch das Prinzip Security by Design eine wichtige Rolle in der Cyberhärtung von Weltrauminfrastrukturen: Der IT-Backbone verteilter Intelligenz im All sollte nicht nur als Datenpipeline gesehen werden, sondern muss auch als gesamte Betriebs- und Sicherheitsarchitektur über Orbit-, Link- und Bodensegment hinweg gedacht werden. On Board-Processing reduziert zwar Downlink-Engpässe und Abhängigkeiten vom Bodensegment, verlagert aber zugleich kritische Funktionen (Vorverarbeitung, Priorisierung, Entscheidungslogik) in eine Umgebung, in der Cyber- und elektromagnetische Angriffe möglich sind.

Denkt man dies weiter und stellt europäische technologische Souveränität in den Fokus, so kommt

[4] ESA – ESA oversees in-orbit cybersecurity demonstration

man schnell zu Supply-Chain-Sicherheit und Hardware-Trust: Ein sicherer IT-Backbone endet nicht bei Verschlüsselung, Zero Trust und Monitoring. In verteilten Weltraumsystemen muss sich Vertrauenswürdigkeit auch auf die technische Lieferkette erstrecken. Software, Firmware, Field Programmable Gate Arrays (FGPAs), Funkmodule, Beschleuniger, Sensorik, Kryptokomponenten und Bodeninfrastruktur können selbst Träger von Schwachstellen, Manipulationen oder unerwünschten Abhängigkeiten sein. Damit rückt Supply-Chain-Sicherheit von einem Beschaffungsthema in den Kern der Sicherheitsarchitektur.

Erforderlich sind deshalb belastbare Herkunfts- und Integritätsnachweise für kritische Komponenten, abgesicherte Build- und Updateprozesse, kontrollierte Softwarelieferketten, signierte Artefakte, reproduzierbare Builds sowie klare Freigabe- und Austauschprozesse für Hardware und Firmware. Wo immer möglich, sollten Hardware Root of Trust, sichere Boot-Ketten, kryptographisch abgesicherte Updatemechanismen und manipulationsresistente Konfigurationspfade vorgesehen werden. Ziel ist, dass nicht nur der laufende Betrieb überwacht wird, sondern bereits die technische Herkunft und Unverfälschtheit der eingesetzten Komponenten überprüfbar bleiben.

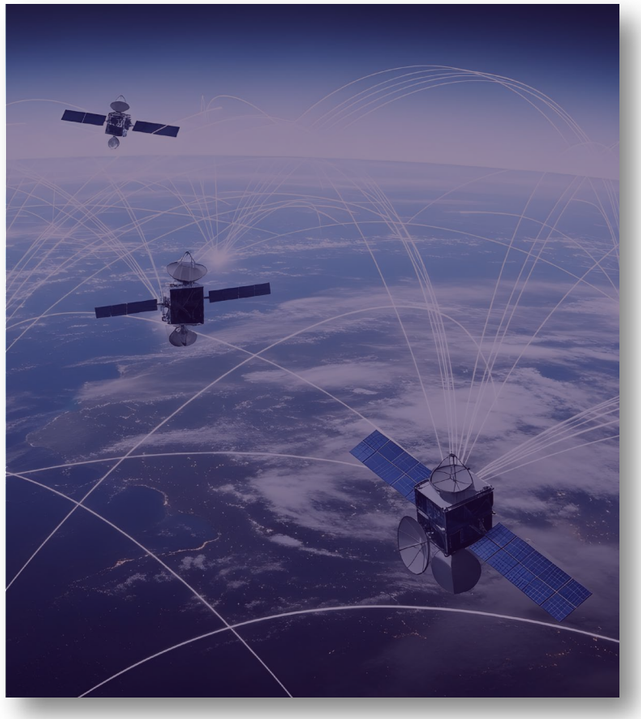
Gerade in militärischen Weltraumsystemen besteht andernfalls das Risiko, dass Sicherheitslücken, verdeckte Manipulationen oder strategische Abhängigkeiten erst im Betrieb sichtbar werden – zu einem Zeitpunkt also, in dem Austausch, Nachhärtung oder Ersatz nur eingeschränkt möglich sind. Supply-Chain-Sicherheit und Hardware-Trust sind daher keine Ergänzung, sondern Voraussetzung für Security by Design.

Ein sicherer IT Backbone folgt konsequent dem Prinzip Security by Design und setzt vor allem auf folgende technische Komponenten:

- Zero Trust Architecture (ZTA): Keinem Nutzer, keinem Gerät und keiner Kommunikation wird per se vertraut – auch nicht innerhalb des Systems. Stattdessen wird jede Interaktion kontinuierlich authentifiziert, autorisiert und über-

wacht, unabhängig davon, ob sie aus einem Satelliten, einer Bodenstation oder einem Missionsnetz kommt – never trust, always verify. In aktuellen Forschungs- und Architekturansätzen für Satelliten- und Raumfahrtinfrastrukturen wird ZTA zudem als zentrale Grundlage gesehen, um klassische Schutzmechanismen zu ergänzen, etwa in Kombination mit KI-gestützter Anomalieerkennung (siehe nächsten Punkt) oder abgesicherten Inter-Satellite-Links, um Jamming, Spoofing und laterale Bewegungen von Angreifern wirksam einzudämmen.

- KI-gestützte Threat Intelligence: Traditionelle Cybersicherheitsmethoden, wie Verschlüsselung und Intrusion Detection Systeme, reichen nicht aus, um hochentwickelten Cyberangriffen – beispielsweise Signalstörungen (Jamming), Spoofing und adversariellen KI-Angriffen – wirksam zu begegnen. Daher sind Sicherheitsframeworks der nächsten Generation, die KI-gestützte Anomalieerkennung integrieren, entscheidend für den Schutz von Satellitennetzen.
- Inter-Satellite-Links: Optische Verbindungen zwischen Satelliten ermöglichen es ihnen, direkt miteinander zu kommunizieren, ohne permanent auf Bodenstationen angewiesen zu sein. Dadurch entstehen dezentrale, vernetzte Systeme, die auch bei Ausfall einzelner Knoten oder Bodeninfrastruktur weiterhin funktionsfähig bleiben können – ein wesentlicher Beitrag zur Robustheit und Verfügbarkeit von Raumfahrtsystemen. Für die Architektur bedeutet das vor allem Redundanz und Autonomie: Daten können über alternative Pfade innerhalb der Konstellation weitergeleitet werden, Missionsfunktionen lassen sich verteilen und zeitkritische Informationen müssen nicht zwingend den Umweg über die Erde nehmen.
- Postquantenkryptographie: Diese Technologie adressiert gezielt das Risiko, dass heute aufgezeichnete Kommunikationsdaten in Zukunft – etwa durch leistungsfähige Quantenrechner – nachträglich entschlüsselt werden könnten. Architektonisch ermöglicht Quantenkryptographie vor allem vertrauenswürdige Schlüsselverteilung als Fundament für robuste Verschlüsselung, ohne sich dauerhaft auf die rechnerische Sicherheit klassischer Algorithmen verlassen zu müssen. In verteilten, hochvernetzten Systemen wie Satelliten- und Weltraumnetzen stärkt sie damit die Integrität und Vertraulichkeit zentraler Datenflüsse, selbst unter der Annahme technologischer Durchbrüche auf Angreiferseite. Der Beitrag von Quantenkryptographie liegt weniger in der Abwehr aktueller Angriffe als in der Absicherung der langfristigen Funktionsfähigkeit und Vertrauenswürdigkeit digitaler Systeme über Jahrzehnte hinweg.



5. SOUVERÄNES DATENMANAGEMENT

Mit der Verlagerung von Rechenleistung, Missionslogik und Vorverarbeitung in den Orbit wird Datenmanagement von einer unterstützenden IT-Funktion zu einer architekturprägenden Kernfähigkeit. Eine resiliente deutsche Weltraumarchitektur braucht daher nicht nur sichere Kommunikationsverbindungen und robuste Plattformen, sondern auch ein souveränes Datenmanagement, das Verfügbarkeit, Vertraulichkeit, Integrität, Nachweisbarkeit und kontrollierte Nutzbarkeit über Orbit-, Link- und Bodensegment hinweg gewährleistet. Im Kern geht es darum, dass Deutschland und seine Partner nicht nur Sensoren und Satelliten betreiben, sondern die entstehenden Datenströme, Metadaten, Modelle, Ableitungen und Entscheidungsgrundlagen jederzeit kontrolliert, regelbasiert und missionsorientiert beherrschen. Wie eingangs beschrieben lassen sich Daten gegenwärtig nicht in der Geschwindigkeit bewegen, wie sie generiert werden. Hier kann ein gewisses Prozessieren der Daten durch maschinelles Lernen an Bord von Satelliten unterstützen.

Souveränität bedeutet in diesem Zusammenhang nicht Autarkie um jeden Preis. Gemeint ist vielmehr die Fähigkeit, für unterschiedliche Datenarten und Missionskontexte selbst bestimmen zu können, wo Daten erzeugt, verarbeitet, gespeichert, geteilt, angereichert, gelöscht und wiederhergestellt werden. Dazu gehören insbesondere Sensordaten, Lagebilder, Telemetriedaten, Kommandodaten, Betriebsdaten, Sicherheitsereignisse, Trainingsdaten für KI-Modelle, Modellartefakte sowie abgeleitete Produkte für Führung, Aufklärung und Wirkung. Ohne ein solches Ordnungsmodell besteht das Risiko, dass zwar technisch leistungsfähige Konstellationen entstehen, die daten- und betriebsseitig jedoch in proprietäre Teilwelten zerfallen.

1. Erforderlich ist zunächst eine klare Datenklassifikation. Nicht alle Daten haben denselben Schutzbedarf, dieselbe Lebensdauer oder denselben operativen Wert. Rohdaten aus Sensoren, verdichtete Missionsdaten, Lageprodukte, Betriebs- und Diagnoseinformationen sowie sicherheitsrelevante Telemetrie müssen unterschiedlich behandelt werden. Für jede Klasse sind Regeln für Speicherung, Weitergabe, Aufbewahrung, Replikation und Löschung festzulegen. Erst dadurch wird es möglich, Datenflüsse so zu steuern, dass bandbreitenkritische Orbit-Boden-Verbindungen entlastet, hochkritische Daten besonders geschützt und operativ weniger relevante Daten nachgelagert verarbeitet werden können.

2. Souveränes Datenmanagement braucht Provenance und Nachweisbarkeit. In verteilten Architekturen muss jederzeit nachvollziehbar bleiben, woher Daten stammen, auf welcher Plattform sie erzeugt wurden, welche Verarbeitungsschritte stattgefunden haben, welche Modelle oder Algorithmen zum Einsatz kamen und welche Version einer Software oder eines Modells eine bestimmte Ableitung erzeugt hat. Dies ist nicht nur für die technische Fehleranalyse wichtig, sondern auch für militärische Verlässlichkeit, forensische Aufklärung, Akkreditierung und die Vertrauenswürdigkeit von Entscheidungsunterstützung. Daten ohne belastbare Herkunfts- und Verarbeitungskette sind in einem hochdynamischen Operationsraum nur eingeschränkt nutzbar.

3. Datenmanagement muss föderiert und interoperabel gedacht werden. In der Anfangsphase mag es genügen, dass einzelne Konstellationen jeweils separat betrieben werden. Langfristig ist dies jedoch weder effizient noch resilient. Eine multiorbitale Gesamtarchitektur verlangt, dass unterschiedliche Konstellationen, Missionssysteme, Bodenstationen und Führungsnetze Daten über standardisierte Schnittstellen austauschen können. Dazu gehören gemeinsame Metadatenmodelle, semantische Beschreibungen, versionierte Datenverträge sowie klare Freigabe- und Nutzungsregeln. Ziel ist keine zentralistische Einheitsplattform, sondern ein föde-

riertes Datenökosystem, in dem Systeme eigenständig bleiben, aber kontrolliert miteinander kooperieren können.

4. Es muss festgelegt werden, wo Compute und Storage platziert werden. Ein Teil der Datenverarbeitung wird aus Bandbreiten- und Zeitgründen künftig im Orbit erfolgen. Ein anderer Teil gehört aus Gründen der Langzeitverfügbarkeit, Zusammenführung, weitergehenden Analyse oder rechtlichen Nachweisführung in sichere Bodeninfrastrukturen und Rechenzentren. Souveränes Datenmanagement heißt deshalb auch, eine bewusste Architekturentscheidung über Datenlokalität zu treffen: Welche Daten bleiben on board, welche werden in regionalen oder nationalen Rechenzentren verarbeitet, welche werden repliziert, und welche dürfen in partner- oder cloudgestützte Umgebungen ausgeleitet werden? Diese Fragen sind kein reines Infrastrukturthema, sondern berühren unmittelbar Souveränität, Einsatzfähigkeit und Sicherheit.

5. Datenmanagement muss den Umgang mit KI explizit umfassen. Wenn KI-Modelle im Orbit Daten filtern, priorisieren oder klassifizieren, dann werden nicht nur Daten, sondern auch Modelle selbst zu schutzwürdigen und missionskritischen Objekten. Trainingsdaten, Modellversionen, Gewichte, Inferenzprotokolle und Qualitätsmetriken müssen daher ebenfalls Gegenstand der Governance sein. Nur so lässt sich nachvollziehen, warum ein System eine bestimmte Beobachtung priorisiert, verworfen oder als Bedrohung eingestuft hat. Damit wird souveränes Datenmanagement zugleich zur Grundlage einer belastbaren AI-Governance.

6. Souveränes Datenmanagement ist eng mit Cloud-, Rechenzentrums- und Betriebsmodellen verknüpft. Die Architektur braucht leistungsfähige Datenplattformen am Boden, um große Datenmengen aufzunehmen, zu korrelieren, zu sichern und in Produkte für militärische und politische Entscheidungen zu überführen. Gleichzeitig muss vermieden werden, dass die Datenhoheit faktisch an externe Betreiber, proprietäre Plattformen oder außereuropäische Abhängigkeiten verloren geht. Souveränität bedeutet deshalb auch, dass Schlüssel, Metadatenkontrolle, Datenhaltungsregeln, Auditfähigkeit und Exitfähigkeit nicht nur vertraglich, sondern technisch abgesichert werden. Neueste Data Centric Security (DCS) Lösungsarchitekturen können hierzu einen wertvollen Beitrag leisten.

Zusammengefasst ist souveränes Datenmanagement der Mechanismus, der verteilte Weltraumsysteme beherrschbar macht. Es verbindet Datenklassifikation, Provenance, Interoperabilität, Speicher- und Compute-Placement, KI-Governance und sichere Datenräume zu einem Ordnungsrahmen, der operative Nutzung und strategische Souveränität zusammenführt. Ohne ein solches Modell droht die künftige Weltraumarchitektur in eine Vielzahl leistungsfähiger, aber datenpolitisch und technisch fragmentierter Insellösungen zu zerfallen.

6. EINFÜHRUNG UND BESCHAFFUNG NEUER TECHNOLOGIEN

Der beschriebene Paradigmenwechsel ist nicht nur eine Frage neuer Technologien, sondern in der Umsetzung auch eine Frage der Beschaffungs- und Managementlogik. Die Frage stellt sich, wie Bundeswehr, etablierte Unternehmen, Start-ups und die Wissenschaft erfolgreich in einem leistungsstarken Verteidigungsökosystem zusammenarbeiten können. Diese Frage wird vor dem Hintergrund der Zeitenwende viel diskutiert. Neue Formate und schnellere Beschaffung werden bereits effektiv umgesetzt. Im Folgenden seien zu dieser Diskussion anlässlich des eingangs beschriebenen Paradigmenwechsels ein paar Gedanken aus dem Bereich Weltraum beigesteuert.

Wenn sich Steuerung, Datenverarbeitung und Entscheidungslogik zunehmend vom Bodensegment in den Orbit verlagern, verändern sich Innovationszyklen grundlegend: Fähigkeiten werden weniger durch seltene Hardwaregenerationen bestimmt, sondern durch kontinuierliche Softwareweiterentwicklung, Updates und datengestützte Verbesserungen. Gleichzeitig zielt die Logik von Software Defined Defence (SDD) genau auf diesen Taktwechsel: weg von starren, hardwarezentrierten Modernisierungspfaden, hin zu einer fortlaufenden Fähigkeitsentwicklung über Software. Daraus folgt zwingend: Eine resiliente Weltraumarchitektur lässt sich nicht mehr „einmalig beschaffen", sondern muss als dynamisches System of Systems (SoS) über Jahre aktiv gemanagt und iterativ weiterentwickelt werden.

Das Thema SDD, bzw. der Fokus auf Software, bedeutet in der Konsequenz jedoch, dass eine deutsche Industriepolitik darauf abzielen muss, dass IT-Unternehmen die Rüstungsindustrie, konkret die Hersteller von Hardware, unterstützen können. Traditionell kommt die Software an Bord von Satelliten überwiegend von den Satellitenherstellern selbst. Drei Gegebenheiten erfordern an dieser Stelle ein Umdenken:

1. Die Raumfahrtindustrie hat nicht das nötige Personal, um die immensen und bislang ungekannten Auftragsvolumen, die in den kommenden Jahren in der militärischen Raumfahrt anfallen werden, abzuarbeiten.
2. Eine resiliente Weltraumarchitektur erfordert auch eine resiliente industrielle Basis. Resilienz (und idealerweise Effizienz) steigt mit einer effektiven Arbeitsteilung.
3. Gerade im Bereich intelligenter Systeme können sowohl Satellitenbauer als auch die Rüstungsindustrie vom Know-how von IT-Unternehmen profitieren. Auch der Bereich der Cybersicherheit und die Absicherung durch quantencomputerresistente Algorithmen sind vielversprechende Felder der Zusammenarbeit. Der Logik von SDD folgend ist die IT-Industrie kein reiner Zulieferer, sondern Mit-Enabler neuer militärischer Fähigkeiten – gemeinsam mit der Raumfahrt- und der Rüstungsindustrie.

Wenn Fähigkeiten auch durch SDD, d. h. über kontinuierliche Softwareweiterentwicklung, Updates und datengestützte Verbesserungen, entstehen, dann reicht die klassische Logik des Beschaffens, der Abnahme und der Betriebsphase nicht mehr aus. Militärische Fähigkeiten sind nicht mehr nur „einmalig beschaffbar", sondern müssen über Jahre aktiv gemanagt und iterativ weiterentwickelt werden. Die Abnahme wird nicht länger ein einmaliger Meilenstein sein, sondern ein fortlaufender Prozess aus Test, Verifikation, Sicherheitsbewertung und gestaffelter Ausbringung. Entsprechend muss die Bundeswehr (und das Ökosystem) nicht nur Technologie, sondern auch einen verlässlichen Mechanismus einkaufen, der jede neue Softwareversion schnell, sicher und nachweisbar in Nutzung

bringt – ohne dass jeder Patch ein Mini-Neubeschaffungsprojekt wird.

Die Fähigkeit, neue Technologien schnell einzuführen, darf jedoch nicht auf Kosten technischer und strategischer Vertrauenswürdigkeit gehen. Gerade softwaredefinierte Weltraumsysteme erhöhen die Zahl kritischer Komponenten, Lieferanten und Updatepfade. Beschaffung muss deshalb nicht nur Leistungsdaten und Preis bewerten, sondern auch Herkunft, Integrität, Austauschbarkeit und langfristige Beherrschbarkeit zentraler Komponenten.

Dies betrifft insbesondere Halbleiter, On-Board-Compute, Beschleuniger, Kommunikationsmodule, Kryptokomponenten, Softwarebausteine und cloudnahe Plattformdienste. Wo kritische Fähigkeiten auf wenige ausländische oder proprietäre Quellen konzentriert sind, entstehen potenziell strategische Abhängigkeiten. Eine resiliente Weltraumarchitektur erfordert daher auch eine resiliente industrielle Basis: diversifizierte Lieferketten, technische Nachweisführung, abgesicherte Integrationsprozesse, definierte Ersatzstrategien und – wo sicherheitspolitisch erforderlich – europäische oder nationale Vertrauensanker für besonders kritische Kernkomponenten.

Eine weiterführende Frage ist, wie Forschung und Industrie zusammenwirken, ohne dass Innovation in Prototypen stecken bleibt oder Jahre vergehen, bis neue Technologien von der Truppe genutzt werden können. Der technologische Kern des Paradigmenwechsels – On-Board Compute, autonome Verarbeitung, KI gestützte Entscheidungen und neue Betriebslogiken im Orbit – erfordert eine stärkere Kette von der Forschung (Methoden, Sicherheit, Robustheit) über Demonstratoren bis zur Serienfähigkeit. Praktisch heißt das: Beschaffung sollte stärker „vom Experiment zur Skalierung" denken. Gleichzeitig müssen Rüstungs- und Satellitenhersteller mit der IT-Industrie effektiv zusammenarbeiten. Denn die größten Risiken liegen selten nur in der Technologie selbst, sondern in Integration, Betrieb, Security by Design und der Überführung in ein belastbares Betriebsmodell, das mit der verteilten Intelligenz im All Schritt hält.

UNSER BEITRAG

Der Paradigmenwechsel hin zu softwaredefinierten, verteilten Weltraumsystemen erfordert Akteure, die Raumfahrt, Digitalisierung und Sicherheit integriert denken und umsetzen können. Genau hier setzt die neue und gemeinsame Aufstellung von Sopra Steria und der CS Group in DS² an: Defence, Security & Space. Sie verbindet mehr als 40 Jahre operative Raumfahrtexpertise mit über 20 Jahren Erfahrung in der Beratung des Rüstungsbereichs: Security-by-Design- und Projektberatung in allen Phasen der projektbezogenen Bedarfsdeckung und Nutzung der Bundeswehr. Wir sind BSI-zertifizierter IT-Sicherheitsdienstleister des Bundes und beraten die Bundeswehr seit Jahren bei der Akkreditierung von Systemen durch die DEUmilSAA. Die Softwarelösungen der CS Group unterstützen in Europa Weltraummissionen von Missionsdesign und -betrieb bis hin zur sicheren Verarbeitung und Nutzung von Weltraumdaten.

Damit sind Sopra Steria und CS Group nicht nur Technologielieferanten, sondern auch Systemintegratoren für die nächste Generation von Weltraumarchitekturen: Architekturen, die auf Modularität, offene Schnittstellen, kontinuierliche Updates und Security by Design setzen und so genau jene Resilienz, Skalierbarkeit und Geschwindigkeit ermöglichen, die der neue sicherheitspolitische und technologische Kontext verlangt.

Der besondere Mehrwert von Sopra Steria und CS Group liegt in der Fähigkeit, übergreifende Zielarchitekturen und belastbare Operating Models für softwaredefinierte Weltraumsysteme zu entwerfen und umzusetzen. Im Mittelpunkt steht das systemische Zusammenspiel von Orbit Segment, Link Segment und Ground Segment – ergänzt um Security Architekturen, Daten- und Souveränitätsmodelle, DevSecOps Mechanismen und den späteren Betrieb. Damit adressiert DS² genau jene Integrationsherausforderungen, die in verteilten, multiorbitalen Architekturen zum kritischen Erfolgsfaktor werden.

Ein zentraler Differenzierer ist die Rolle als Security- und Akkreditierungs-Enabler. Sopra Steria und CS Group sind in der Lage, Technologievorhaben nicht nur technisch umzusetzen, sondern sie von Beginn an so zu gestalten, dass daraus akkreditierbare, betreibbare und auditierbare Systeme entstehen. Gerade in softwaredefinierten Weltraumarchitekturen, in denen kontinuierliche Updates, KI basierte Funktionen und verteilte Betriebsmodelle zusammenkommen, wird diese Fähigkeit zum entscheidenden Hebel zwischen Innovation und realer Nutzbarkeit.

Ein weiterer Schwerpunkt unserer Dienstleistungen liegt auf föderierten Daten- und Souveränitätsmodellen. Sopra Steria beherrscht methodisch die Gestaltung souveräner Daten , Cloud- und Security Architekturen, die es erlauben, verteilte Weltraumsysteme interoperabel, nachvollziehbar und kontrollierbar zu betreiben. Gerade im Kontext multiorbitaler Architekturen und sicherheitskritischer Missionen wird damit die Grundlage geschaffen, Daten, Modelle und Entscheidungsprozesse über Organisations- und Systemgrenzen hinweg kontrolliert zu nutzen, ohne Souveränität oder Nachweisbarkeit zu verlieren.

ANSPRECHPARTNER

DR. CAROLIN BUSCH
Senior Managerin Defence & Space
carolin.busch@soprasteria.com

DR. SPENCER ZIEGLER
Chief Operating Officer
spencer.ziegler@cs-soprasteria.com

KONTAKT

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg

T. 040 22703-0
E. info.de@soprasteria.com
W. www.soprasteria.com

CS Group
ECOS Office Center Darmstadt /
Campus Berliner Allee
Berliner Allee 65
64295 Darmstadt

T. 06151 3975-257
W. www.cs-soprasteria.com

sopra steria

CS
a Sopra Steria company