

Resiliente Space-Infrastruktur

Vorschläge für eine sichere und leistungsfähige europäische Space-Infrastruktur

bitkom

Resiliente Space-Infrastruktur

Ausgangslage

Weltraumgestützte Dienste sind zu einer zentralen Grundlage für Wirtschaft, Staat und Verteidigung geworden. Kommunikation, Navigation, präzise Zeitmessung und Erdbeobachtung sichern kritische Prozesse weit über den Raumfahrtsektor hinaus. Gleichzeitig steigen die Risiken durch Cyberangriffe, Störmaßnahmen auf der Erde und im Weltraum, technische Ausfälle sowie geopolitische und industrielle Abhängigkeiten.

Bitkom-Bewertung

Deutschland und Europa haben die strategische Bedeutung resilienter Space-Infrastrukturen erkannt. Entscheidend ist nun, Resilienz und Verfügbarkeit konsequent Ende-zu-Ende zu denken: von Satelliten und Bodensegmenten über Daten- und Cloud-Infrastrukturen bis zu Lieferketten und der Einbindung kommerzieller Kapazitäten. Regulierung und Beschaffung müssen dabei Sicherheit hinsichtlich Verfügbarkeit, Vertraulichkeit, Integrität, Wettbewerb und Innovationsfähigkeit miteinander verbinden.

Unser Ziel ist eine leistungsfähige europäische Space-Infrastruktur, die kritische Dienste auch unter Störungen, in Krisen und hybriden Bedrohungslagen verlässlich bereitstellt. Dafür müssen Resilienz durch Space und die Resilienz der Space-Infrastruktur gemeinsam gestärkt werden.

Das Wichtigste

Für eine resiliente Space-Infrastruktur müssen technologische, regulatorische und industriepolitische Maßnahmen zusammengedacht werden. Aus Sicht des Bitkom sind drei Punkte besonders entscheidend:

- **Space sektorenübergreifend in der Resilienzplanung verankern:** Mit dem KRITIS-Dachgesetz ist Weltraum als kritischer Sektor anerkannt. Nun müssen auch die Abhängigkeiten anderer kritischer Sektoren von Satellitenkommunikation, Positionsbestimmung, Navigation, Zeitmessung (Position, Navigation & Timing, PNT), Erdbeobachtung und weiteren Space-Diensten systematisch in Risikoanalysen, Notfallplanung und öffentliche Beschaffung einfließen.
- **Resilienz Ende-zu-Ende verankern:** Cybersicherheit und Resilienz by Design, robuste Lieferketten, Degraded Operations (leistungsreduzierter Betrieb) sowie schnelle Wiederherstellung und die stetige Anpassungsfähigkeit müssen bereits bei Entwicklung, Beschaffung und Betrieb mitgedacht und regelmäßig erprobt werden.
- **Europäische Fähigkeiten und kommerzielle Kapazitäten skalieren:** gestaffelte Programme in wiederkehrenden Tranchen, Anbieterdiversität durch wettbewerbliche Vergabemodelle sowie Vorhalteverträge für Infrastruktur und Dienste, der Staat als Ankerkunde, interoperable Schnittstellen sowie verfügbare europäische Start-, Cloud- und On-Orbit-Kapazitäten schaffen planbare Nachfrage, stärken die industrielle Basis und erhöhen die strategische Handlungsfähigkeit.

Inhalt

1 Space als kritische digitale Infrastruktur 4

2 Die doppelte Resilienzaufgabe: Resilienz durch Space und Resilienz der Space-Infrastruktur 5

3 Kritische Space-Dienste und ihre Anwendungsfelder 7

4 Anforderungen an eine resiliente Ende-zu-Ende-Architektur 9

5 Space in zentralen Wirtschafts- und Anwendungssektoren 14

6 Handlungsempfehlungen 16

1 Space als kritische digitale Infrastruktur

Die Space-Infrastruktur ist heute keine Spezialinfrastruktur einzelner Raumfahrtakteure mehr, sondern Teil der digitalen Basisinfrastruktur moderner Volkswirtschaften. Kommunikations-, Navigations-, Zeit- und Erdbeobachtungsdienste unterstützen Prozesse in den Bereichen Telekommunikation, Energieversorgung, Mobilität, Landwirtschaft, Industrie, staatliche Handlungsfähigkeit und militärische Operationen. Ihre Verfügbarkeit ist somit nicht nur eine Frage der technischen Leistungsfähigkeit im Weltraum, sondern auch eine Voraussetzung für die Resilienz und Effizienz zahlreicher anderer Infrastrukturen und Sektoren auf der Erde.

Mit der fortschreitenden Digitalisierung und Integration von Space nimmt diese Abhängigkeit weiter zu. Zeitkritische, automatisierte und sicherheitsrelevante Prozesse sind immer stärker von präzisen Daten, zuverlässigen Positionsinformationen und stabilen Kommunikationswegen abhängig. Ein Ausfall weltraumgestützter Dienste kann sich deshalb kaskadenartig auf die Bereiche Telekommunikation, Mobilität und Logistik, Energie, Verwaltung, Industrie und Verteidigung auswirken. Aktuelle Konflikte und hybride Bedrohungslagen zeigen zugleich, dass Raumfahrtinfrastrukturen nicht nur unverzichtbare Fähigkeiten bereitstellen, sondern selbst zunehmend strategische Zielobjekte darstellen. Ihre Resilienz ist somit nicht nur eine sektorale Aufgabe der Raumfahrtpolitik, sondern auch ein Bestandteil nationaler Resilienzvorsorge. Space-Infrastrukturen müssen entsprechend als Teil einer vernetzten kritischen Digitalarchitektur betrachtet werden. Besonders deutlich wird diese Abhängigkeit beim Positioning, Navigation & Timing (PNT). Satellitennavigationssysteme liefern nicht nur Positionsdaten, sondern auch hochpräzise Zeitinformationen und stellen damit eine gemeinsame Referenz für Telekommunikationsnetze, Energieversorgung, Finanztransaktionen, Rechenzentren, Industrieprozesse und zahlreiche IT-Systeme bereit. Ein temporärer Ausfall oder die Manipulation solcher Signale kann deshalb sektorübergreifende Kaskadeneffekte auslösen.

Mit zunehmender Automatisierung gewinnt dies zusätzlich an Bedeutung: Der automatisierte Straßen-, Schienen-, Schiffs- und Drohnenverkehr benötigt Position und Zeit nicht nur zur Orientierung, sondern auch als sicherheitskritische Grundlage für operative Entscheidungen. Zugleich verändert die Verbindung von terrestrischen und nicht-terrestrischen Netzen die Rolle der Space-Infrastruktur. Non-Terrestrial Networks (NTN), insbesondere neue Low-Earth-Orbit-(LEO)-Satellitennetze, werden stärker mit terrestrischen Kommunikationsinfrastrukturen verzahnt. Dies betrifft unter anderem Anwendungen im Automotive-Bereich, den Güterverkehr, Gefahrenabwehr und Sicherheitsvorsorge sowie satellitengestützte Notrufsysteme. Satellitenkommunikation wird damit zunehmend Bestandteil einer integrierten Kommunikationsarchitektur. Insbesondere dort, wo terrestrische Netze nicht verfügbar, gestört oder zerstört sind, kann sie einen zusätzlichen Kommunikationspfad bereitstellen.

Erdbeobachtung leistet auf andere Weise einen Beitrag zur Resilienz. Ihr Mehrwert liegt insbesondere in Frühwarnungen, Lagebildern und Monitoring. Mithilfe von Erdbeobachtungs- und Wetterdaten können Veränderungen in den Bereichen

Landwirtschaft, Klimawandel, Waldbranderkennung, Energieversorgung und kritische Infrastrukturen frühzeitig erkannt werden. Auf dieser Grundlage können datenbasierte Entscheidungen getroffen werden. Die zugrunde liegenden Fähigkeiten können sowohl wirtschaftliche als auch staatliche und sicherheitsrelevante Anwendungen unterstützen.

Mit der steigenden Zahl von LEO-Satelliten und anderen Objekten im Weltraum gewinnen Space Domain Awareness und Space Traffic Management zunehmend an Bedeutung. Kollisionsrisiken, Weltraumschrott und gezielte Störungen können nämlich den Betrieb einzelner Satelliten ebenso beeinträchtigen wie die langfristige Nutzbarkeit von Orbits. Eine resiliente Space-Infrastruktur setzt daher aktuelle und präzise Lageinformationen voraus. Diese ermöglichen eine frühzeitige Gefahrenerkennung sowie ressourcenschonende Ausweich- bzw. Schutzmaßnahmen und gewährleisten eine möglichst lange und ungestörte Missions- und Nutzungsdauer.

Schließlich wird Resilienz auch durch industrielle und geopolitische Abhängigkeiten bestimmt. Ob Space-Infrastruktur auch in Krisen und hybriden Bedrohungslagen verlässlich betrieben und bei Bedarf wiederhergestellt werden kann, hängt von der Verfügbarkeit kritischer Komponenten, dem Zugang zum Weltraum, ausreichenden Produktionskapazitäten sowie belastbaren Wartungs- und Lieferketten ab. Eine resiliente europäische Space-Infrastruktur benötigt daher neben technologischer Leistungsfähigkeit auch eine wettbewerbsfähige, verfügbare und dauerhaft tragfähige industrielle Basis.

2 Die doppelte Resilienzaufgabe: Resilienz durch Space und Resilienz der Space-Infrastruktur

Resilienz im Weltraum hat zwei eng miteinander verbundene Dimensionen. Einerseits können weltraumgestützte Dienste andere Sektoren widerstandsfähiger machen. Andererseits müssen die dafür benötigten Space-Systeme selbst gegen Störungen, Angriffe und Ausfälle abgesichert sein. Space-Dienste können ihre Funktion als Resilienzanker für Wirtschaft, Staat und Sicherheit damit nur erfüllen, wenn die zugrunde liegende Infrastruktur selbst auch unter erschwerten Bedingungen funktionsfähig bleibt.

Resilienz durch Space entsteht insbesondere dort, wo weltraumgestützte Dienste zusätzliche und möglichst unabhängige Kommunikations-, Beobachtungs- oder Referenzebenen schaffen. Satellitenkommunikation kann alternative Kommunikationspfade bereitstellen, wenn terrestrische Netze ausfallen oder im Krisenfall überlastet sind. Erdbeobachtungsdaten können Lagebilder und Frühwarninformationen liefern. PNT stellt Positions- und Zeitinformationen für

Verkehrs-, Energie-, Telekommunikations-, Finanz- und Industrieprozesse bereit. Gerade dort, wo terrestrische Redundanzen nur mit hohem Aufwand oder aufgrund geografischer Bedingungen kaum realisierbar sind, können Space-Dienste die Widerstandsfähigkeit erheblich stärken.

Resilienz der Space-Infrastruktur setzt wiederum voraus, dass nicht nur einzelne Satelliten oder andere orbitale Infrastrukturen, sondern die gesamte Leistungskette und deren Architektur widerstandsfähig und adaptiv ausgelegt wird. Für den Aufbau und den Betrieb resilienter Ende-zu-Ende-Wertschöpfungsketten werden umfassende logistische Fähigkeiten und ein systematischer Transfer erprobter Logistik-Lösungen und -Technologien benötigt. Resilienz muss zu jedem Zeitpunkt des Lebenszyklus im Systemdesign angelegt sein – von Entwicklung und Beschaffung über Fertigung, Lagerung, Betrieb und Wartung bis hin zur Modernisierung und Wiederherstellung sowie aktiven Entsorgung ausgedienter Satelliten aus der endlichen Anzahl von Umlaufbahnen. Dazu gehören physischer Schutz und Cybersicherheit ebenso wie belastbare Lieferketten, eine funktionierende Logistik, interoperable Systeme, Redundanzen und tragfähige Betriebsmodelle.

Eine zentrale Rolle spielt dabei Diversität. Kritische Dienste sollten möglichst nicht von einer einzigen technischen Quelle, einem einzelnen Betreiber oder einer einzelnen Infrastruktur abhängen. Bei PNT-Anwendungen können beispielsweise verschiedene Satellitensysteme, perspektivisch unterschiedliche Weltraumarchitekturen und terrestrische Referenzen miteinander kombiniert und validiert werden. Für den Zeitdienst können mehrere Satellitensignale durch terrestrische Quellen und lokale Oszillatoren ergänzt werden. Unterschiedliche technische und physische Pfade verringern das Risiko, dass eine einzelne Störung das gesamte System beeinträchtigt. Auch Satellitenkommunikation profitiert von mehrschichtigen Architekturen. Redundanz und Vernetzung im Orbit, Nutzung verschiedener Frequenzbänder, geografisch verteilte Bodeninfrastrukturen und flexible Netzsteuerung können dazu beitragen, einzelne Ausfälle und breite Angriffe zu kompensieren. Terrestrische und nicht-terrestrische Kommunikationswege sollten deshalb als komplementäre Bestandteile einer resilienten Gesamtnetzarchitektur verstanden werden. Resilienz bedeutet dabei nicht, jeden Ausfall verhindern zu können. Systeme müssen auch darauf vorbereitet sein, unter eingeschränkten Bedingungen weiterzuarbeiten. Degraded Operations, leistungsreduzierter Betrieb, sichere Rückfallebenen, Notfallverfahren und Wiederanlaufmechanismen müssen bereits im Vorfeld definiert, technisch ermöglicht und regelmäßig erprobt werden. Neben Prävention und Adaption gehört damit auch die Fähigkeit, Auswirkungen zu begrenzen und ausgefallene Leistungen schnell wiederherzustellen, zu einer resilienten Architektur.

Dabei müssen Resilienzkonzepte neben technischen Risiken auch hybride Bedrohungen wie Cyberangriffe, physische Sabotage, Manipulationen von Lieferketten oder Insider-Risiken berücksichtigen. Technische, organisatorische und sicherheitsbezogene Maßnahmen müssen daher gemeinsam gedacht werden. Die doppelte Resilienzaufgabe geht deshalb über rein technische Anforderungen hinaus. Sie umfasst gleichermaßen Technologie, Betrieb, Governance und industrielle Leistungsfähigkeit und Verfügbarkeit. Industrielle Leistungsfähigkeit und Verfügbarkeit setzen Skalierungsfähigkeit auf der Erde voraus. Im Space-Bereich herrscht vielfach noch Manufaktur-Betrieb vor. Die Industrie muss schnell

zur Industrialisierung befähigt werden. Dazu gehören eine belastbare Logistik, funktionierende Lieferketten und das Vorhalten von Produktionskapazitäten sowie die Einbindung weiterer Unternehmen, insbesondere auch des Mittelstands, entlang der Lieferketten. Eine wettbewerbsfähige europäische Space-Industrie, belastbare Wertschöpfungsketten und abrufbare Wiederherstellungskapazitäten sind ebenso Teil der Resilienz wie Cybersicherheit und technologische Diversität.

3 Kritische Space-Dienste und ihre Anwendungsfelder

Weltraumgestützte Dienste unterscheiden sich hinsichtlich ihrer Funktion, Kritikalität und damit ihrer Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit. Für eine resiliente Space-Infrastruktur ist daher entscheidend, welchen Beitrag einzelne Dienste zur Widerstandsfähigkeit leisten und welche Anforderungen sich daraus für ihren verlässlichen Betrieb ergeben.

Satellitenkommunikation

Satellitenkommunikation ist ein zentraler Bestandteil resilienter und hochverfügbarer digitaler Infrastrukturen. Sie kann u. a. Kommunikationswege und damit Führungsfähigkeit für Behörden und Einsatzkräfte bereitstellen, als Ergänzung zu terrestrischen Mobilfunknetzen dienen sowie maritime und aeronautische Kommunikation ermöglichen. Für Energieanlagen, Industrie oder andere Infrastrukturen an abgelegenen Standorten kann sie einen zusätzlichen Kommunikationskanal schaffen. In Regionen mit eingeschränkter terrestrischer Infrastruktur kann Satellitenbreitband darüber hinaus Konnektivität gewährleisten. Systeme im Low Earth Orbit (LEO), Medium Earth Orbit (MEO) und Geostationary Earth Orbit (GEO) verfügen dabei über unterschiedliche Stärken und sollten als komplementäre Bestandteile einer resilienten Kommunikationsarchitektur verstanden werden. Multi-Orbit-Ansätze können diese unterschiedlichen Fähigkeiten kombinieren und gemeinsam mit Multi-Provider-Architekturen zusätzliche Kommunikationspfade, Redundanzen und flexible Kapazitäten bereitstellen.

Positioning, Navigation & Timing

PNT ist eine weitreichende Querschnittsfähigkeit. Präzise Zeitinformationen ermöglichen unter anderem die Synchronisation von Telekommunikations-, Energie-, Finanz- und IT-Infrastrukturen. Positions- und Navigationsdienste sind für Mobilität, Logistik, Landwirtschaft und automatisierte Prozesse von zentraler Bedeutung. Mit der zunehmenden Automatisierung sicherheitskritischer Navigations- und Steuerungsprozesse steigen auch die Anforderungen an die Verlässlichkeit von PNT.

Eine zentrale Voraussetzung für resiliente PNT-Dienste ist die Fähigkeit, Störungen und Manipulationen wie Jamming, Spoofing und Signaldegradation frühzeitig zu erkennen. Anti-Jamming-Technologien, geeignete Antennensysteme und Verfahren zur Signalauthentifizierung können dabei ebenso einen Beitrag leisten wie die Nutzung mehrerer unabhängiger Quellen. Ergänzende terrestrische Zeit- und Ortsreferenzen sowie lokale Systeme können helfen, zeitlich begrenzte Unterbrechungen zu überbrücken.

Für sicherheitskritische Anwendungen reicht eine möglichst genaue Positionsinformation allein nicht aus. Erforderlich sind zusätzlich Aussagen über die Integrität und Vertrauenswürdigkeit der Positionslösung sowie eine rechtzeitige Warnung, wenn die zugesicherte Qualität nicht mehr gewährleistet werden kann. Dies ist insbesondere für automatisierten Straßen-, Schienen-, Schiffs- und Drohnenverkehr relevant.

Erdbeobachtung und Wetterdaten

Erdbeobachtungs- und Wetterdaten ermöglichen Frühwarnung, Lagebilder, Monitoring und datenbasierte Entscheidungen. Sie unterstützen unter anderem Katastrophenschutz, Landwirtschaft, Wasserwirtschaft, Energieversorgung, Infrastrukturmonitoring, Lieferkettenmanagement sowie Umwelt- und Sicherheitsanwendungen. Der besondere Resilienzbeitrag liegt in der frühzeitigen Erkennung von Veränderungen, Nachverfolgung und der Möglichkeit, auch großräumige Entwicklungen zu beobachten. Solche Entwicklungen können auch in Regionen stattfinden, die mit luft- oder erdgebundenen Sensoren nicht erreichbar sind. Darüber hinaus gewinnen Erdbeobachtungsdaten für ressortübergreifende Lagebilder zunehmend an Bedeutung. Sie unterstützen Behörden und Sicherheitsorganisationen bei der frühzeitigen Erkennung von Naturereignissen, Infrastrukturstörungen, Umweltveränderungen und sicherheitsrelevanten Entwicklungen. Damit werden sie zu einem wichtigen Baustein datengetriebener Entscheidungs- und Führungsprozesse.

Space Domain Awareness und Space Traffic Management

Mit der intensiven Nutzung der Erdorbits und der Zunahme von Weltraumschrott wächst der Bedarf an aktuellen und präzisen Informationen über Objekte und Aktivitäten im Weltraum. Space Domain Awareness und Space Traffic Management tragen dazu bei, Kollisionsrisiken frühzeitig zu erkennen, Satelliten zu schützen und Störungen besser einzuordnen. Damit unterstützen sie nicht nur die Sicherheit einzelner Missionen, sondern auch die langfristige Nutzbarkeit orbitaler Infrastruktur. Dazu gehört auch die Schaffung einer Aufklärungsfähigkeit, die bewusst herbeigeführte kritische Annäherungen als Provokation und Angriff erkennen kann und Gegenmaßnahmen ergreifen kann.

Sichere Daten- und Auswertungsdienste

Der Wert von Space-Daten entsteht zunehmend durch ihre schnelle Verarbeitung, Kombination und Analyse. Sichere Cloud- und Rechenzentrumskapazitäten, KI-gestützte Auswertung sowie klar geregelte und rollenbasierte Zugänge sind deshalb Bestandteil einer resilienten Space-Infrastruktur. Dies gilt unabhängig davon, ob diese Kapazitäten on-premises, in souveränen Private-Cloud-

Umgebungen, in eingestuften Netzen oder bei kommerziellen Cloud-Anbietern betrieben werden. Missions-, Telemetrie- und Erdbeobachtungsdaten müssen dabei selbst gegen Verlust, Manipulation und Verschlüsselung durch Ransomware geschützt sein, etwa durch unveränderbare (immutable) Datenkopien, Verschlüsselung ruhender Daten und getrennte Wiederherstellungsumgebungen.

Zunehmend rückt dabei auch die orbitale Datenverarbeitung in den Fokus resilienter Architekturen. Die Verarbeitung von Missions-, Telemetrie- und Nutzlastdaten direkt im Orbit — auf standardisierten, updatefähigen Rechenplattformen an Bord von Satelliten oder auf Raumstationen — ermöglicht es, kritische Auswertungsschritte unabhängig von terrestrischen Rechenzentren und Kommunikationsverbindungen durchzuführen. Dies erhöht die Widerstandsfähigkeit gegenüber Störungen der Bodeninfrastruktur und verkürzt Latenzzeiten bei zeitkritischen Anwendungen. Souveräne orbitale Dateninfrastruktur ergänzt damit On-Premises- und Private-Cloud-Umgebungen und eingestufte Netzlösungen um eine weitere, inhärent unabhängige Schicht — und sollte in der Förder- und Sicherheitsarchitektur entsprechend berücksichtigt werden.

Responsive Space und On-Orbit-Services

Zur Resilienz gehört schließlich die Fähigkeit, ausgefallene Kapazitäten möglichst schnell wiederherzustellen. Verfügbarer Zugang zum Weltraum, Ersatzkapazitäten, standardisierte Satellitenplattformen sowie Wartungs-, Inspektions- und weitere On-Orbit-Services können dazu beitragen, Wiederherstellungszeiten zu verkürzen. Dadurch lassen sich zugleich kritische Abhängigkeiten von einzelnen Start- und Serviceanbietern reduzieren. Hierbei sind insbesondere auch Startplätze in Europa zu identifizieren, die mehr als nur eine Orbitalbahn erreichen können und ein niedrigeres Bedrohungspotential durch Angriffe aufweisen.

4 Anforderungen an eine resiliente Ende-zu-Ende-Architektur

Ende-zu-Ende-Architektur als Ausgangspunkt

Eine resiliente Space-Infrastruktur muss als Ende-zu-Ende-System, von der Mission bis zu den Nutzenden, gedacht werden. Entscheidend ist nicht nur die Widerstandsfähigkeit des Weltraumsegments, sondern das Zusammenspiel aus Weltraumsegment, Bodensegment, inklusive des Zugangs zur und der Nutzung der Daten- und Cloud-Infrastruktur, bis hin zur operativen Steuerung und zum Lieferkettenmanagement. Schwachstellen in einem Systemelement können die Funktionsfähigkeit des gesamten Systems beeinträchtigen.

Die Enterprise-Architektur bildet den Rahmen. Eine resiliente Space-Infrastruktur entsteht nicht aus einzelnen Systemen, sondern aus einer abgestimmten

Enterprise-Architektur. Sie beschreibt Fähigkeiten, Prozesse, Daten, Anwendungen und Technologien über alle Segmente hinweg. Sicherheit ist dabei ein Architekturprinzip und kein nachträglich aufgesetztes Modul. Referenzarchitekturen, gemeinsame Bausteine und definierte Architekturprinzipien schaffen die Grundlage dafür, dass alle Segmente konsistent geplant und betrieben werden.

Ein einfaches Beispiel zeigt, warum das so ist. Ein Satellitenbetreiber verbindet Satelliten, Bodenstationen, Cloud-Dienste und Nutzerterminals. Ist eines dieser Glieder schwach geschützt, kann eine angreifende Person darüber in das Gesamtsystem eindringen. Das gilt auch dann, wenn der Satellit selbst gut gesichert ist. Cybersicherheit darf deshalb nicht erst am Satelliten ansetzen. Sie muss die gesamte Kette abdecken.

Diversität und Anpassungsfähigkeit statt Einzelabhängigkeit

Resilienz entsteht deshalb nur, wenn diese Komponenten gemeinsam und vernetzt abgesichert, interoperabel und auf Ausfälle vorbereitet sind. Zentrale Architekturprinzipien sind Diversität und Adaptierbarkeit statt Einzelabhängigkeit und statischer Konfiguration. Für kritische Anwendungen sollten unterschiedliche Systeme, Orbits, Betreiber und Übertragungsmedien miteinander kombiniert werden. Multi-Orbit- und Multi-Provider-Ansätze können das Risiko reduzieren, dass der Ausfall eines einzelnen Anbieters oder einer einzelnen Systemarchitektur zum Ausfall des gesamten Dienstes führt. Diese Prinzipien sind als Architekturanforderungen in der Enterprise-Architektur zu verankern. Sie gelten für alle Segmente gleichermaßen.

Terrestrische Backup-Verfahren ergänzen diese Architektur. Die Anforderungen sollten zugleich risikobasiert ausgestaltet werden: Nicht jeder Dienst benötigt denselben Schutzgrad. Für staatliche, sicherheitsrelevante und KRITIS-nahe Anwendungen sind höhere Verfügbarkeits-, Sicherheits- und Business-Continuity-Anforderungen sachgerecht als für weniger kritische Dienste. Eine Enterprise-Architektur macht Abhängigkeiten transparent. Dazu gehören Datenflüsse, Schnittstellen, Dienstleister, Standorte und Lieferwege. Erst mit diesem Gesamtbild lässt sich bewerten, welche Störungen sich kaskadieren und wo Redundanzen fehlen. Fachliche Anforderungen aus Projekten und Programmen werden so mit Referenzmustern verbunden. Entscheidungen über Schutzbedarf, Redundanz und Wiederherstellung werden dadurch nachvollziehbar und vergleichbar.

Resiliente Space-Infrastruktur betrifft gleichermaßen Bundeswehr, Bundesbehörden, KRITIS-Unternehmen, Industrie und Partner. Hierfür ist die Anschlussfähigkeit entscheidend. Gemeinsame Schnittstellen, Interoperabilität und abgestimmte Architekturprinzipien ermöglichen ein sicheres Zusammenwirken der Systeme unterschiedlicher Akteure. Eine enge zivil-militärische Zusammenarbeit trägt zudem dazu bei, dass Space-Dienste auch bei Störungen ressortübergreifend nutzbar bleiben.

Bodensegment als physisch erreichbares Schutzobjekt

Das **Bodensegment** ist ein besonders wichtiger Bestandteil dieser Ende-zu-Ende-Perspektive. Redundante Bodenstationen und Kontrollstationen zum Betrieb und Flug der Satelliten, geschützte Strom- und Netzanschlüsse sowie geografisch verteilte Bodenstationen können dazu beitragen, den Betrieb auch bei lokalen Ausfällen fortzuführen. Energieeffiziente und kompakte IT- und Speichersysteme erhöhen die Durchhaltefähigkeit von Boden- und Kontrollstationen im Notstrombetrieb. Verlegefähige Bodensegmente sollten Daten auch ohne Anbindung an zentrale Rechenzentren lokal verarbeiten und sichern können (Disconnected Operations). Unterschiedliche Glasfaserwege und die Möglichkeit, Kommunikation bei Bedarf über andere Standorte zu führen, reduzieren lokale Single Points of Failure. Da Bodensegmente physisch erreichbar sind, müssen sie besonderen Cyber-, Sabotage- und Ausfallrisiken entsprechend mindestens unter Einhaltung vergleichbarer Sicherheits- und Resilienzanforderungen wie beim Weltraumsegment abgesichert werden.

Softwaredefinierte Systeme und Veränderungsfähigkeit

Gleichzeitig verändert sich die technische Architektur der Raumfahrt. **Softwaredefinierte Raumfahrtsysteme** ermöglichen es, Funktionen eines Satelliten nach dem Start stärker anzupassen, zu erweitern oder zu optimieren. Signalverarbeitung, Teile der Missionslogik oder zusätzliche Anwendungen können dadurch aktualisiert werden, ohne für jede Änderung neue Hardware in den Orbit bringen zu müssen. Dies erhöht Flexibilität, Nutzungsdauer und potenziell auch Wirtschaftlichkeit. Der Paradigmenwechsel eröffnet zugleich die Möglichkeit, funktionale Sicherheit und Cybersicherheit stärker *by design* zu verankern. Hochsichere Betriebssysteme, geeignete Mikroelektronik und offene beziehungsweise kontrollierbare Komponenten können dabei einen Beitrag leisten. Jede Softwareaktualisierung ist jedoch zugleich ein möglicher Angriffsweg. Die zunehmende Updatefähigkeit erhöht deshalb die Anforderungen an eine robuste und geschützte Software- und Systemarchitektur. Updates müssen signiert, geprüft und nachvollziehbar eingespielt werden.

Modulare und offene Systemarchitekturen schaffen Veränderungsfähigkeit. Durch die Entkopplung von Hardware und Software sowie klar definierte, offene Schnittstellen können einzelne Komponenten leichter ausgetauscht und weiterentwickelt werden. Softwaredefinierte Ansätze ermöglichen es zudem, Funktionen anzupassen und Schutzmaßnahmen nachzurüsten. Dadurch steigen Anschlussfähigkeit und Veränderungsfähigkeit der Systeme. Gleichzeitig muss die Architektur sicher und beherrschbar bleiben. Austauschbare Komponenten benötigen daher klar definierte Schnittstellen, eine nachvollziehbare Herkunft und geprüfte Updates.

Cybersecurity by Design und sichere Systemarchitektur

Cybersecurity by Design ist deshalb eine Grundvoraussetzung resilienter Space-Systeme. Satelliten, Bodenstationen, Kommunikationsverbindungen, Datenverarbeitung und Terminals für Nutzende müssen von Beginn an Teil eines

durchgängigen Sicherheitskonzepts sein. Eine nachträgliche Ergänzung reicht nicht aus, da die Nachrüstung von Sicherheitsfunktionen insbesondere bei bereits im Einsatz befindlichen Satelliten technisch und wirtschaftlich aufwendig ist. Ein frühzeitig definiertes, durchgängiges Sicherheitskonzept verhindert zudem, dass einzelne Schwachstellen die gesamte Systemarchitektur gefährden. In der Enterprise-Architektur sollte Sicherheit daher Bestandteil jeder Referenzarchitektur sein. Dazu gehören kontinuierliches Monitoring von Netzen, Steuerungs- und Telemetriedaten, die frühzeitige Erkennung von Anomalien und klar definierte Reaktionsprozesse. Bodenstationen, Netze und Steuerungssysteme sollten dabei möglichst kontinuierlich auf Angriffsindikatoren und Manipulationen überwacht werden. KI-gestützte Verfahren können bei der Erkennung ungewöhnlicher Muster und der Priorisierung von Warnungen unterstützen, sollten jedoch Teil einer nachvollziehbaren und abgesicherten Betriebsarchitektur sein. Insbesondere müssen automatisiert erzeugte Warnungen überprüfbar bleiben und dürfen nicht ungeprüft zu Eingriffen in den Systembetrieb führen.

Für Kommando- und Kontrollverbindungen bietet sich ein Zero-Trust-Ansatz an, bei dem Zugriffe nicht allein aufgrund einer bestehenden Verbindung als vertrauenswürdig gelten. Zugriffsberechtigungen sollten unabhängig von ihrer Herkunft überprüft und auch bei bereits etablierten Verbindungen kontinuierlich neu bewertet werden. Dies reduziert zugleich das Risiko, das von kompromittierten Partnersystemen ausgehen kann. Auf dem Satelliten selbst können Maßnahmen wie Secure Boot mit Hardware-Vertrauensanker, signierte und verschlüsselte Kommandos, eine Trennung von Steuerungs- und Nutzlastsystemen sowie schlanke Intrusion-Detection-Funktionen die Widerstandsfähigkeit erhöhen. Kryptografisch abgesicherte Kommandos sollten dabei auch verhindern, dass gefälschte oder unzulässig wiederholte Befehle angenommen werden. Bei Anomalien sollte ein Wechsel in einen sicheren Betriebszustand möglich sein. Ebenso relevant ist die Fähigkeit, nach einer Kompromittierung vertrauenswürdige Systemzustände wiederherzustellen. Soweit technisch möglich, sollte eine solche Wiederherstellung auch ohne eine bestehende Verbindung zur Bodenstation möglich sein, damit sie nicht von einer möglicherweise gestörten oder kompromittierten Kommunikationsverbindung abhängig ist.

Automatisierte Wiederherstellung und sichere Systemarchitektur

Moderne cloud-native Bodensegmente können die Resilienz erhöhen, indem ausgefallene oder gestörte Dienste automatisch neu gestartet oder auf andere Systeme verlagert werden. Diese Fähigkeit ersetzt jedoch keine kontinuierliche Sicherheitsüberwachung. Wird ein kompromittierter Dienst lediglich neu gestartet, kann ein Angriff unentdeckt fortbestehen.

Automatisierte Wiederherstellung und Sicherheitsarchitektur müssen deshalb zusammen geplant und implementiert werden. Softwarekomponenten sollten auf Schwachstellen geprüft, laufende Systeme überwacht und Netze innerhalb der Infrastruktur segmentiert werden. KI-gestützte Verfahren können bei der Erkennung von Auffälligkeiten unterstützen; weitreichende Eingriffe in den Systembetrieb müssen jedoch nachvollziehbar bleiben und menschliche Kontrolle ermöglichen.

Für eine sichere Wiederherstellung müssen zudem vertrauenswürdige und manipulationsgeschützte Kopien von Daten und Konfigurationen verfügbar sein. Andernfalls werden Dienste zwar neu gestartet, arbeiten aber auf kompromittierten oder verschlüsselten Datenbeständen weiter.

Eine durchgängige Enterprise-Architektur sollte die technischen und organisatorischen Sicherheitsfunktionen miteinander verbinden. Dazu gehören klare Schnittstellen zwischen Überwachung, Wiederherstellung und Lagebildern sowie eindeutig geregelte Verantwortlichkeiten. Informationen über Störungen im Weltraumsegment, Angriffe auf Bodensegmente und Manipulationen in Lieferketten sollten zusammengeführt werden, damit Zusammenhänge und mögliche Auswirkungen auf andere Systeme frühzeitig erkannt werden können.

Positioning, Navigation & Timing (PNT)

Für PNT-Systeme kommen spezifische technische Anforderungen hinzu. Eine resiliente Architektur sollte unterschiedliche Signalquellen und ausreichend diverse Frequenzbereiche nutzen. Anti-Jamming und Spoofing-Erkennung sowie Signalauthentifizierung sollten bei sicherheitskritischen Anwendungen nicht als optionale Zusatzfunktionen betrachtet werden. Erkannte Störungen sollten zudem in zeitgerechte, digitale Warn- und Integritätsinformationen für betroffene Nutzende und Systeme überführt werden. Wichtig sind außerdem klar definierte sichere Zustände, wenn die Integrität einer Positions- oder Zeitinformation nicht mehr gewährleistet werden kann. Das Ausbleiben einer Warnung darf in einem sicherheitskritischen System nicht automatisch als Nachweis einer korrekten Positionslösung interpretiert werden.

Verantwortung, Governance und unabhängige Überwachung

Resilienz benötigt neben Technik eine **klare operative und organisatorische Verantwortung**. Die Rollen von Diensteanbietern, Infrastrukturbetreibern und Systemintegratoren müssen definiert sein. Dazu gehören dokumentierte Leistungs- und Verfügbarkeitsanforderungen sowie klare Melde-, Eskalations- und Wiederanlaufprozesse. Für erkannte Bedrohungen sollten zudem vordefinierte Reaktionsabläufe und, wo sinnvoll, automatisierte Erstmaßnahmen vorgesehen werden. Bedrohungen und Vorfälle müssen nachvollziehbar dokumentiert und entlang klar definierter Prozesse gemeldet und bearbeitet werden können. Es sollten zudem geeignete physische und personelle Schutzmaßnahmen vorgesehen werden. Dazu gehören der Schutz kritischer Standorte wie Boden- und Kontrollstationen, ausreichende Redundanzen, geeignete Zutritts- und Berechtigungskonzepte sowie personelle Vorsorge für Krisen- und Störungssituationen.

Für sicherheitskritische Anwendungen sollten unabhängige Überwachungs- und Bewertungsfunktionen vorgesehen werden, die organisatorisch und technisch von den Infrastrukturbetreibern getrennt sind. Diese können insbesondere dazu beitragen, Fehler oder Manipulationen zu erkennen, die innerhalb der eigenen Betriebsstrukturen unentdeckt bleiben. Degraded Operations und alternative Betriebsverfahren sollten nicht nur dokumentiert, sondern regelmäßig praktisch erprobt werden.

Sicherheit der Lieferkette

Schließlich ist die **Lieferkette** Teil der Sicherheitsarchitektur. Angriffe und Manipulationen können bereits bei der Herstellung von Hardware- und Softwarekomponenten erfolgen, lange bevor ein System in Betrieb geht. Kritische Komponenten und Software müssen nachvollziehbar, überprüfbar und gegen Manipulation geschützt sein. Sicherheitsstandards und Qualifizierungsverfahren, die offen, transparent und diskriminierungsfrei entwickelt werden, können Vertrauen zwischen Herstellern, Betreibern und staatlichen Nutzenden schaffen, ohne den Markteintritt neuer Anbieter zu erschweren. Eine resiliente Lieferkette setzt zudem eine diversifizierte Lieferantenlandschaft voraus, in der neben etablierten Anbietern auch KMU und Startups angemessene Zugangsmöglichkeiten erhalten. Gleichzeitig müssen kritische Single-Source-Abhängigkeiten reduziert und ausreichend alternative Bezugs- und Wartungsmöglichkeiten geschaffen werden. Industrie- und Sicherheitspolitik sind an dieser Stelle unmittelbar miteinander verbunden.

5 Space in zentralen Wirtschafts- und Anwendungssektoren

Die Bedeutung resilienter Space-Infrastrukturen zeigt sich insbesondere in den Sektoren, deren operative Prozesse von Kommunikation, Zeit, Position oder aktuellen Lageinformationen abhängen. Dabei greifen häufig mehrere Space-Dienste ineinander. Entscheidend ist daher, sektorspezifische Abhängigkeiten zu identifizieren und bei Resilienzplanung, Notfallvorsorge und Wiederherstellung gemeinsam zu berücksichtigen.

Für **digitale Infrastruktur und Telekommunikation** ist Satellitenkommunikation zunehmend eine Ergänzung terrestrischer Netze. Satellitenkommunikation und insbesondere neue LEO- und Multi-Orbit-Architekturen können Backhaul, Notfallkonnektivität und die Versorgung abgelegener Standorte unterstützen. Mit der zunehmenden Integration von NTN in Mobilfunk- und perspektivisch 5G-/6G-Architekturen verschwimmt die bisherige Trennung zwischen terrestrischer und satellitengestützter Kommunikation. Entscheidend ist nicht, bestehende Netze durch Satelliten zu ersetzen, sondern hybride Architekturen zu schaffen, die im Störungsfall auf alternative Kommunikationspfade zurückgreifen können. Auch der Schutz der Frequenznutzung ist ein zentraler Resilienzfaktor. Frequenzdiversität und alternative Kommunikationspfade können dazu beitragen, die Steuerung der Satelliten sowie die Übertragung von Nutzdaten und den Zugriff darauf auch bei Störungen abzusichern.

Im Bereich **Mobilität, Luftfahrt und Logistik** kommen mehrere Abhängigkeiten zusammen. PNT unterstützt Navigation, Tracking und automatisierte Systeme; Satellitenkommunikation ermöglicht Kommunikation jenseits terrestrischer Abdeckung; Wetter- und Erdbeobachtungsdaten unterstützen Planung,

Lagebewertung und Entscheidungsprozesse. Insbesondere für automatisierte Mobilität wird eine verlässliche, integritätsüberwachte Positions- und Zeitinformation zunehmend sicherheitskritisch. Gleichzeitig gewinnen NTN-Anwendungen im Automotive-Bereich an Bedeutung, etwa für Notruf, Verkehrssicherheitstechnik, Überwachungs- und Kommunikationsfunktionen. Der steigende Güterverkehr verstärkt die Bedeutung zuverlässiger Verbindungen und Positionsdaten zusätzlich.

Für **Manufacturing und Industrie** liegt die besondere Bedeutung von Space-Diensten in der zunehmenden Vernetzung und Automatisierung von Produktionsprozessen. Präzise Zeit- und Positionsinformationen können unter anderem für synchronisierte Systeme, autonome Intralogistik und standortübergreifende Prozesse relevant sein. Erdbeobachtungsdaten können ergänzend Informationen über Produktionsstandorte, Transportwege oder Veränderungen im Umfeld kritischer Anlagen liefern. Entscheidend ist, solche Space-Daten über standardisierte Schnittstellen mit vertretbarem Aufwand in bestehende Industrie-, Produktions- und Logistiksysteme integrieren zu können.

Im Bereich **Digital Farming und Ernährungssicherheit** tragen PNT, Wetter- und Erdbeobachtungsdaten zur Präzisionslandwirtschaft, zum Boden- und Vegetationsmonitoring und zur Bewirtschaftung von Wasserressourcen bei. Wetter-, Erdbeobachtungs- und PNT-Daten unterstützen die datenbasierte Anpassung an Klima- und Produktionsrisiken. Ein niedrigschwelliger Zugang zu Daten sowie zu geeigneten Analyse-, Beratungs- und Cloud-Services kann die Nutzung dieser Fähigkeiten verbreitern.

Für **Smart City und Smart Region** sind Geoinformation, Stadt- und Regionalplanung, Katastrophenschutz und der Betrieb kommunaler Infrastrukturen relevante Anwendungsfelder. Erdbeobachtung kann Lagebilder und Planungsinformationen verbessern; Satellitenkommunikation kann einen zusätzlichen Kommunikationsweg für Krisen- und Notfallsituationen bereitstellen. Einfach zugängliche Plattformen, gemeinsame Datenpools und interoperable Standards können dazu beitragen, diese Fähigkeiten auch auf kommunaler Ebene nutzbar zu machen.

Für **Energie, öffentliche Sicherheit und Katastrophenschutz** ist die Kombination unterschiedlicher Space-Dienste besonders relevant. Zeitinformationen unterstützen die Synchronisation technischer Netze, Satellitenkommunikation kann abgelegene Anlagen oder Einsatzkräfte anbinden, und Erdbeobachtungsdaten ermöglichen Lagebilder und Frühwarnung. Gerade im Katastrophenfall ist entscheidend, dass Space-Dienste auch dann zur Verfügung stehen, wenn lokale Infrastruktur bereits beeinträchtigt ist.

Für **Sicherheit, Verteidigung und DefTech** sind gehärtete und geschützte Kommunikation & Führungsfähigkeit, Lagebilder, Aufklärung, PNT, Space Domain Awareness sowie schnelle Wiederherstellungsfähigkeiten von starker Bedeutung. Moderne Streitkräfte sind auf verlässliche und abgesicherte Space-Dienste angewiesen. Zugleich können kommerzielle und Dual-Use-Anbieter einen wichtigen Beitrag leisten. Vergabe-, Sicherheits-, Einstufungs- und Vertragsmodelle sollten daher so ausgestaltet sein, dass kommerzielle Anbieter, die definierte Sicherheits- und Zuverlässigkeitsanforderungen (etwa Sicherheitsüberprüfungen,

Zertifizierungen und IT-Sicherheitsnachweise) erfüllen, in transparenten Verfahren frühzeitig eingebunden, Kapazitäten bereits in Friedenszeiten vorgehalten und ihre Leistungen auch in Krisen- und Verteidigungsszenarien verlässlich verfügbar gemacht werden können.

6 Handlungsempfehlungen

Um die Resilienz weltraumgestützter Dienste und der zugrunde liegenden Space-Infrastruktur nachhaltig zu stärken, braucht es einen kohärenten politischen und regulatorischen Rahmen. Dabei müssen Sicherheitsanforderungen, technologische Souveränität, Wettbewerbsfähigkeit und Innovationsfähigkeit gemeinsam gedacht werden. Aus Sicht des Bitkom sind insbesondere folgende Maßnahmen erforderlich:

1. **Space als horizontale kritische digitale Infrastruktur verstehen.** Space-Infrastruktur sollte in Regulierung, Strategie, Förderpolitik, Resilienzplanung und öffentlicher Beschaffung konsequent als sektorübergreifende Infrastruktur berücksichtigt werden. Dabei müssen neben Bodeninfrastrukturen auch die Abhängigkeiten anderer kritischer Sektoren von Satellitenkommunikation, PNT, Erdbeobachtung und weiteren Space-Diensten in Risikoanalysen und Notfallplanungen berücksichtigt werden. Satellitenkommunikation zusammen mit terrestrischer Kommunikation sollte systematisch als sich ergänzende Kommunikationsoption für kritische Anwendungen eingeplant werden.

2. **Hybride Bedrohungen gegen Space-Infrastrukturen systematisch adressieren.** Bund und Länder sollten Space-Infrastrukturen stärker in bestehende Resilienz-, Sicherheits- und KRITIS-Konzepte integrieren. Hierzu gehören Sensibilisierung, Training, Schutzmaßnahmen gegen Cyberangriffe, Sabotage, Insider-Risiken und Lieferkettenmanipulationen ebenso wie abgestimmte Lagebilder und Meldewege zwischen Wirtschaft und Staat.

3. **Schutzanforderungen harmonisieren und regulatorische Doppelstrukturen vermeiden.** EU Space Act, NIS2, KRITIS-Dachgesetz, weitere europäische Resilienzvorgaben und nationale Strategien sollten so zusammenspielen, dass Schutzanforderungen eindeutig sind, ohne parallele Berichts-, Prüf- und Nachweispflichten aufzubauen. Anforderungen sollten sich am tatsächlichen Risiko und an definierten Ergebnissen wie Verfügbarkeit, Wiederherstellungsfähigkeit und Sicherheitsniveau orientieren. Dabei sollten bestehende europäische und internationale Normen sowie etablierte Konformitätsbewertungsverfahren berücksichtigt werden, soweit sie geeignet sind, harmonisierte Anforderungen und Nachweise zu unterstützen und regulatorische Doppelstrukturen zu vermeiden. Jegliche

Regulatorik ist zudem insbesondere auch kritisch daraufhin zu prüfen, inwiefern Innovations- und Wettbewerbsfähigkeit hierdurch beeinträchtigt werden. Sensible Betriebsinformationen wie Netzwerktopologien und Kapazitätsdaten benötigen zugleich einen angemessenen Vertraulichkeitsschutz.

4. **Resilienz und Cybersicherheit by Design als überprüfbare Beschaffungs- und Förderkriterien für verteidigungsrelevante Projekte verankern.** Cybersicherheit, Business Continuity, Resilienz in der Architektur, sichere Datenverarbeitung und -speicherung, nachweisbare Wiederherstellungsfähigkeit von Daten mit definierten Wiederherstellungszeiten, Supply-Chain-Sicherheit, Degraded Operations und Wiederherstellung sollten bereits bei Entwicklung und Beschaffung als überprüfbare Kriterien für verteidigungsrelevante Projekte berücksichtigt werden. Dies betrifft Weltraum-, Link-, Boden- und Segment der Nutzenden mit Daten- und Cloud-Infrastruktur. Für sicherheitskritische Anwendungen sollten Störungserkennung, Authentifizierung und klar definierte Rückfallebenen von Beginn an eingeplant werden. Risikobasierte, möglichst harmonisierte Prüf- und Validierungsverfahren sowie geeignete unabhängige Testmöglichkeiten sollten die Wirksamkeit dieser Anforderungen nachvollziehbar belegen. Hierfür sollten Bedarfsträger, Industrie und Forschung bereits bei der Entwicklung und Erprobung resilienter Space-Technologien eng zusammenarbeiten.

5. **Multi-Orbit-, Multi-Provider- und hybride Netzarchitekturen fördern.** Öffentliche Beschaffung und Förderprogramme sollten Interoperabilität, Anbieterdiversität und Backup-Fähigkeit begünstigen und ein Mindestmaß an Sicherheitsanforderungen für mehr Resilienz im Weltraum vorsehen. Terrestrische und nicht-terrestrische Netze sollten stärker als integrierte Architektur gedacht werden. Standardisierte Schnittstellen und Protokolle sollten die Zusammenarbeit unterschiedlicher Betreiber und Technologien ermöglichen und gleichzeitig so gestaltet sein, dass KMU und Startups direkten Zugang zum Markt behalten. Ebenso sollte eine Verstetigung der Vergaben an konkurrierende Anbieter implementiert werden. Dabei sollte vorrangig auf bestehende, international anschlussfähige Standards zurückgegriffen werden.

6. **Europäische technologische und industrielle Fähigkeiten gezielt stärken.** Europa benötigt robuste, verfügbare und wirksame Fähigkeiten entlang der gesamten Space-Wertschöpfungskette. Dazu gehören Satelliten und Nutzlasten ebenso wie das Boden- und Kontrollsegment, Software, Mikroelektronik, Dateninfrastruktur, Startzugang, Wartung und Wiederherstellung. Für den schnellen Aufbau und den effizienten Betrieb resilienter Ende-zu-Ende-Wertschöpfungsketten werden darüber hinaus umfassende logistische Fähigkeiten und ein systematischer Transfer erprobter Logistik-Lösungen und -Technologien benötigt. Kritische Single-Source-Abhängigkeiten sollten identifiziert und dort reduziert werden, wo

sie ein relevantes Resilienzrisiko darstellen. Europäische und nationale Förder- und Beschaffungsprogramme sowie staatliche Eigenleistungen sollten besser aufeinander abgestimmt werden. Die Vielfalt der Anbieter und der Wettbewerb zwischen ihnen bleiben davon unberührt. Kommerzielle Angebote sollten regelmäßig und systematisch in die Bedarfsdeckung einbezogen werden, sofern sie die Anforderungen an Leistungsfähigkeit, Sicherheit, Verfügbarkeit und Wirtschaftlichkeit erfüllen. Die Auswahl sollte transparenten, leistungsbezogenen Kriterien folgen; hierdurch kann ein nachhaltiges und tragfähiges Ökosystem aufgebaut und Innovation gefördert werden. Zugleich sollten Entwicklung und Einsatz modularer und softwaredefinierter Raumfahrtsysteme gezielt vorangetrieben werden. Rekonfigurierbare und updatefähige Systeme können Innovationszyklen verkürzen und ermöglichen es, Space-Infrastrukturen und -Wertschöpfungsketten schneller an technologische Entwicklungen und veränderte Sicherheitsanforderungen anzupassen.

7. **Mehrjährige Abnahmeverträge ermöglichen und Vergabeverfahren beschleunigen.** Der Staat sollte als Ankerkunde auftreten und etwa über mehrjährige Abnahme- oder Vorhalteverträge planbare Nachfrage für resiliente Space-Infrastrukturen schaffen. Vergabe- und Förderinstrumente sollten so ausgestaltet sein, dass das gesamte Raumfahrtökosystem realistische und direkte Zugangsmöglichkeiten erhält. Schnellere und agile Vergabeverfahren können dabei den Zugang zum Markt erleichtern und gleichzeitig die Planbarkeit der Unternehmen verbessern.

8. **PNT als sektorübergreifende kritische Abhängigkeit behandeln.** Timing und Positionierung auf Basis globaler Navigationssatellitensysteme sollten in der Resilienzplanung von Telekommunikation, Energie, Mobilität, Finanzwesen und weiteren kritischen Bereichen ausdrücklich berücksichtigt werden. Für sicherheitskritische Anwendungen braucht es geeignete Anforderungen an Integrität, Verfügbarkeit, rechtzeitige Warnung und Verantwortlichkeiten. Europäische Programme sollten eine mehrschichtige PNT-Architektur unterstützen und Anforderungen aus automatisierter Mobilität und anderen sicherheitskritischen Anwendungen (Safety-of-Life) frühzeitig einbeziehen. Anti-Jamming, Spoofing-Erkennung und Signalauthentifizierung sollten bei sicherheitskritischen Anwendungen angemessen berücksichtigt werden. Herstellerunabhängige Überwachungs- und Warnfunktionen sollten dabei als eigenständiges Architekturelement mitgedacht werden (»4-Augen-Prinzip«). Zuständigkeiten zwischen Ressorts, Diensteanbietern, Infrastrukturbetreibern und Nutzenden müssen klar geregelt sein.

9. **Bodensegment und Dateninfrastruktur in Förder- und Sicherheitsanforderungen einbeziehen und Datenzugang vereinfachen.** Bodenstationen, Kontrollzentren, Rechenzentren, Datenspeicherung, Cloud-Processing und Zugangsplattformen sind keine nachgelagerten Nebenelemente, sondern wesentliche Bestandteile der Space-Infrastruktur. Sicherheit in der europäischen Datenverarbeitung,

rollenbasierte Zugänge und nachvollziehbare KI-Auswertung sollten stärker bei der Vergabe und Nutzung als Bewertungskriterien berücksichtigt werden. Dies gilt perspektivisch auch für orbitale Datenverarbeitung als Teil des Gesamtstacks: Rechenkapazitäten im Orbit, die Missions- und Nutzlastdaten unabhängig vom terrestrischen Bodensegment verarbeiten können, erweitern die Ende-zu-Ende-Architektur um eine zusätzliche Resilienzebene.

10. **Wiederherstellungskapazitäten und Responsive Space gezielt aufbauen.** Resilienz umfasst nicht nur die Verhinderung eines Ausfalls, sondern auch die Fähigkeit, verlorene Kapazitäten schnell wiederherzustellen. Europäischer Startzugang, europäische Launcher, Ersatzkapazitäten, standardisierte Plattformen, Logistik und On-Orbit-Services sollten deshalb diskriminierungsfrei ausgestaltet und in Resilienzkonzepten berücksichtigt werden. Auch Ersatzteile, Wartungsmöglichkeiten und vorbereitete Vertragsmodelle gehören zu einer belastbaren Wiederherstellungsstrategie. Hierfür braucht es frühzeitig entwickelte und erprobte technische Standards und Schnittstellen, die den schnellen Austausch und die Integration von Systemen, Komponenten und Diensten ermöglichen.

11. **Sektorübergreifende Stresstests und strukturierten Informationsaustausch etablieren.** PNT-Ausfälle, Störungen in der Satellitenkommunikation, Cyberangriffe auf Bodensegmente (einschließlich Ransomware-Szenarien mit Wiederherstellung von Missions- und Betriebsdaten) oder Unterbrechungen von Erdbeobachtungsdaten sollten regelmäßig gemeinsam mit Wirtschaft und staatlichen Stellen geübt werden, wobei der Austausch unternehmensindividueller Geschäftsdaten ausgeschlossen bleibt. Degraded Operations, Notfallverfahren und Wiederanlaufpläne müssen praktisch funktionieren und dürfen nicht nur auf dem Papier bestehen. Ein strukturierter Dialog über Bedrohungs- und Störfallinformationen zwischen den zuständigen staatlichen Stellen und den jeweiligen Betreibern, Herstellern und Nutzenden kann helfen, sektorübergreifende Lagebilder aufzubauen, Störungen und Angriffe früher zu erkennen und Reaktionszeiten zu verkürzen; ein unternehmensübergreifender Austausch wettbewerbsrelevanter Betriebsdaten ist dabei ausgeschlossen.

Bitkom vertritt mehr als 2.300 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e. V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Benjamin Spindeldreier | Junior Manager DefTech & Sicherheit
T +49 30 27576-379 | b.spindeldreier@bitkom.org

Felix Lennart Hake | Bereichsleiter Mobility & Aviation
T + 49 30 27576-243 | f.hake@bitkom.org

Nick Petersen | Manager für digitale Infrastrukturpolitik
M + 49 151 14824830 | n.petersen@bitkom.org

Sven Wagner | Bereichsleiter Smart City
T +49 30 27576-314 | s.wagner@bitkom.org

Verantwortliche Bitkom-Gremien
AK Geoinformation | AK Kommunikationstechnologien | AK Verteidigung
Roundtable New Space

Copyright
Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.