Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cybersicherheit für Weltrauminfrastrukturen

Positionierung des Bundesamts für Sicherheit in der Informationstechnik

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	02.08.2022	Dr. Johanna Niecknig	Erstveröffentlichung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5812
itcssa@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort des Präsidenten

Digitale Kommunikation bestimmt immer mehr unser tägliches Leben. Privat nutzt fast jeder mehr oder weniger das Internet oder digitale Medien zur Organisation seines Tagesablaufs. In der Verwaltung von Bund und Ländern sowie der Wirtschaft ist ohne z.T. global verfügbare digitale Dienste ein effektives und ergebnisorientiertes Arbeiten kaum noch denkbar.

Der Verfügbarkeit und einer angemessenen Sicherheit der Kommunikation und Anwendungen kommt deshalb große, in einigen Bereichen sogar essentielle Bedeutung zu. Diesem Bedarf kann man mit ausschließlich klassischen terrestrischen Infrastrukturen nicht gerecht werden. Vielmehr sind einige Anwendungen nur mittels moderner Satelliteninfrastrukturen realisierbar. Zu nennen sind hier Navigation, Erdbeobachtung und ein global verfügbares Internet-of-Things (IoT) bzw. *Internet from Space*.

Als nationale Cybersicherheitsbehörde sieht sich das BSI auch für die Cybersicherheit von Satelliteninfrastrukturen in der Verantwortung. Insbesondere vor dem Hintergrund der wachsenden Abhängigkeit von Satellitendiensten ist sich das BSI der Bedeutung dieser Verantwortung bewusst.

Ein erster wichtiger Schritt ist die Positionierung zum Thema Cybersicherheit von Satelliten und zugehöriger Infrastrukturen. Die vorliegende Fachpublikation legt den aus technischer Sicht bestehenden strategischen Handlungsbedarf für den Schutz der Cybersicherheit von Weltraumsystemen und zugehörigen Infrastrukturen dar. Daraus abgeleitet ergeben sich konkrete Handlungsfelder und -ziele, denen das BSI durch systematische Entwicklung und Umsetzung geeigneter Maßnahmen begegnen wird. Die Handlungsfelder und Handlungsziele orientieren sich an denen der beschlossenen Cybersicherheitsstrategie für Deutschland, fortgeschrieben für weltraumspezifische Infrastrukturen.

Arne Schönbohm,
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Inhalt

1 Einleitung und Motivation

Die Bedeutung, Komplexität und Abhängigkeit von weltraumgestützten Systemen haben in den letzten Jahren rasant zugenommen, ein stetiges Wachstum ist weiterhin zu prognostizieren. Der Bereich der Satellitenanwendungen mit den drei Hauptfeldern Navigation, Kommunikation und Erdbeobachtung, sticht hierbei besonders hervor; diese sind aus dem täglichen Leben kaum mehr wegzudenken – fallen solche Dienste aus oder sind nicht verfügbar, oder sind die Schutzziele Integrität und Authentizität, teilweise auch Vertraulichkeit der Signale und Daten, der Informationen nicht sichergestellt, kann das einschneidende Auswirkungen haben. Insbesondere verschiedene Sektoren kritischer Infrastrukturen (KRITIS) sind auf satellitengestützte Anwendungen angewiesen. Beispielsweise dienen GNSS[1]-Dienste der Überwachung des Schienen- oder Flugverkehrs, sowie der Synchronisation von Stromnetzen, ebenso ermöglichen sie durch hochpräzise Zeit- und Ortsstempel zuverlässige Finanztransaktionen. Erdbeobachtungssatelliten dienen nicht nur Forschungszwecken, etwa der Erforschung des Klimawandels, sie sind auch eine wesentliche Komponente für das Katastrophenschutzmanagement, etwa zur Koordinierung der Einsatzkräfte, und werden, ebenso wie Kommunikationsdienste, verstärkt zu militärischen Zwecken eingesetzt. Was ein Cybersicherheitsvorfall auf Satellitennetzwerke für Auswirkungen haben kann, zeigte jüngst der Angriff auf das US-Unternehmen VIASAT, welches das Satellitennetzwerk Ka-Sat betreibt. Infolge des Angriffs war der Betrieb mehrerer Tausend deutscher Windkraftanlagen eingeschränkt. Mit dieser sehr knapp gehaltenen Auswahl an Anwendungsbeispielen wird bereits die facettenreiche Bedeutung für Gesellschaft, Wirtschaft, Staat und Wissenschaft verdeutlicht.

Auch im internationalen Kontext wird die Bedeutung Deutschlands als „Weltraumnation“ durch Trends wie etwa Mikrosatelliten und der hierfür geographisch günstigen Lage Deutschlands zunehmen. Eine frühzeitige Positionierung der Bundesrepublik in Bezug auf diesen Trend und seine (IT-)sichere Ausgestaltung hilft, den Standort Deutschland für die Weltraumindustrie attraktiv zu gestalten und eine weltweit führende und damit gestaltende Rolle einzunehmen. Hierdurch kann perspektivisch die Abhängigkeit Deutschlands von anderen Weltraumnationen reduziert werden.

Mit der beschriebenen Zunahme der Bedeutung und Abhängigkeit von Weltraumsystemen geht eine kontinuierliche Verschärfung der Bedrohungslage einher. Neben den Bedrohungen natürlichen Ursprungs / höhere Gewalt (z.B. kosmische Strahlung, Weltraumwetter, Weltraumschrott) sind nicht-natürlichen Bedrohungen Rechnung zu tragen. Dazu zählen vorsätzliche Handlungen (Cyberangriffe, z.B. Hacken der Satelliten-IT-Systeme, Jamming oder Einsatz von Antisatelliten (ASAT)-Waffen in Form von Satelliten, Raketen, terrestrischen Lasersystemen, etc.), organisatorisches Versagen und menschliche Fehlhandlungen (z.B. Konfigurationsfehler), sowie technisches Versagen (z.B. Materialversagen).

Die Notwendigkeit, weltraumgestützte Systeme und die dafür relevanten Assets zu schützen, ist in der Raumfahrtstrategie der Bundesregierung aus dem Jahre 2010 [1] verankert. In Anbetracht des Facettenreichtums des Themas Raumfahrt ist der Schutzbedarf der Systeme (allgemein in Bezug auf die Sicherheit der Systeme, insbesondere auf deren Cybersicherheit) jedoch nur einer von vielen Aspekten in dem gesamten technologisch-wissenschaftlichen, wirtschaftlichen, politischen und zivil-gesellschaftlichen Spielfeld.

Besonders im Kontext der Sicherheit und Verteidigung wurde der Handlungsbedarf in den letzten Jahren jedoch erkannt und der Schutz sicherheitsrelevanter Weltrauminfrastrukturen rückt zunehmend in den Fokus. So ist es ein Ziel der strategischen Leitlinie Weltraum des BMVg [2], die Gesamtheit der potentiellen Bedrohungen für Weltraumsysteme zu erfassen und geeignete Schutzmaßnahmen zu etablieren. In unterschiedlichen ressortübergreifenden Arbeitsgruppen und zivil-militärischen Kooperationen wird die Thematik der Weltraumsicherheit und -verteidigung weiter vorangetrieben und Ansätze zur Regulierung und Koordinierung diskutiert, genannt seien hier der 2019 etablierte Ressortkreis Weltraumnutzung / Weltraumsicherheit, das ressortgemeinsame Weltraumlagezentrum, die Aufstellung des Weltraumkommandos Bundeswehr, das jährlich stattfindende nationale Symposium für Weltraumsicherheit, sowie Konzeption und

[1] GNSS = globales Navigationssatellitensystem

Aufbau eines ressortübergreifenden Koordinierungsstabs Weltraumsicherheit. Ebenso findet eine verstärkte Vernetzung und aktives Einbringen Deutschlands auf internationaler Ebene statt (bspw. CSpO[2], COPUOS[3], PAROS[4]).

Bei den genannten Aktivitäten werden cybersicherheitsrelevante Aspekte als eine mögliche Kategorie von Bedrohungen für Weltraumsysteme implizit mitbedacht, jedoch ist hierzu eine umfassende Betrachtung erforderlich, die ausdrücklich auf jene weltraumspezifischen Assets, Bedrohungen, Risiken mit Cyberbezug fokussiert.

Zum einen ist dies dadurch motiviert, dass der Cyberraum und das Elektromagnetische Spektrum die einzigen gangbaren Wege für einen Angreifer außerhalb befähigter Weltraumfahrernationen sind, eine Aktion gegen Weltraumsysteme vortragen zu können. Angesichts der zunehmenden Digitalisierung und Vernetzung wächst die Angriffsfläche für Cyberattacken; dies gilt auch für Weltraumsysteme. Hinzu kommt eine besondere Attraktivität für einen potentiellen Angreifer [3]: Im Sinne eines Single-Point-of-Failure-Szenarios kann mit vergleichsweise überschaubarem Aufwand ein enormer Schaden erreicht werden. Die Kombination des vergleichsweise hohen Schadenausmaßes und der aufgrund ungenügender Schutzvorkehrungen nicht zu vernachlässigenden Eintrittswahrscheinlichkeit birgt ein besonders ernst zu nehmendes Risiko.

Zum anderen wird in Fachkreisen – auf internationaler als auch nationaler Ebene – immer wieder darauf hingewiesen, dass Kontroll- und Regulierungsmechanismen für Cybersicherheit von Weltraumsystemen oftmals unzureichend formuliert sind oder gänzlich fehlen [4]. Der Cyberangriff auf Satelliten ist eine reelle Bedrohung. Nationale Einrichtungen und Raumfahrt Organisationen werden daher dringend aufgefordert, Strategien für Cybersicherheit im Weltraum zu entwickeln und entsprechende Maßnahmen zu ergreifen [5]. Die Erstellung einer gesamtnationalen Strategie, um zivile, kommerzielle und sicherheitspolitische Aktivitäten ressortgemeinsam zu institutionalisieren, wird auch von der Bundesakademie für Sicherheitspolitik empfohlen [6].

Für zahlreiche Branchen existieren Cybersicherheits-Standards und Regulierungsmechanismen, jedoch ist zu überprüfen, inwieweit diese auch für Infrastrukturen und Systeme im Weltraum anwendbar sind oder aufgrund weltraumspezifischer Besonderheiten anzupassen oder zu erweitern sind. Im Gegensatz zu klassischen terrestrischen Systemen ist dabei auch von Bedeutung, dass die vergleichsweise lange Lebensdauer sowie die extremen Umweltbedingungen eine besondere Sicherheitsarchitektur erfordern. Eine nachträgliche Anpassung der Sicherheitsarchitektur im operativen Betrieb ist derzeit nur begrenzt möglich. Die Möglichkeit eines (feindlichen) physischen Zugriffs auf Satelliten sollte in die Überlegung zu Schutzvorkehrungen einbezogen werden.

In diesem Sinne ist eine systematische Darlegung des Handlungsbedarfs im Rahmen einer raumfahrtspezifischen Cybersicherheits-Strategie und daraus hervorgehenden Mindestanforderungen zwingend erforderlich. Das übergeordnete Leitziel ist die

„Stärkung der Cybersicherheit von Weltrauminfrastrukturen, welche von Relevanz für Staat, Wirtschaft und Gesellschaft sind, zur Sicherstellung der Verfügbarkeit von Diensten über integre, authentische Kommunikation[5].“

Dabei sind insbesondere solche Anwendungen / Systeme im Fokus, bei denen Anforderungen vergleichbar zu denen Kritischer Infrastrukturen (KRITIS) existieren. Der Begriff Weltrauminfrastrukturen umfasst dabei sowohl das Raumsegment als auch das Boden- und Nutzersegment. Aufgrund des maßgeblichen Einflusses auf Gesellschaft, Staat und Wirtschaft liegt der Fokus bei den Betrachtungen auf dem Schutz von Satelliten und zugehörigen Assets (orbitale sowie terrestrische Systeme und Infrastrukturen). Trotz der Vielfalt der

[2] Combined Space Operations (CSpO)-Initiative
[3] United Nations Committee on the Peaceful Uses of Outer Space (COPUOS)
[4] UN-Resolution (A/RES/47/51); The Prevention of an Arms Race in Outer Space (PAROS)
[5] Kommunikation ist als Oberbegriff zu verstehen und bezeichnet jegliche Art des Informationsaustauschs zwischen einem Satelliten und der zugehörigen Bodeninfrastruktur (Up- und Downlink mit Telemetrie- und Telekommandodaten) bzw. zwischen Satelliten (Inter-Satellite-Links). Der Begriff impliziert somit die Übertragung von Steuerbefehlen, Prozessmessdaten, Payload-Daten, die Dienste selbst.

Satellitendienste sind die zu schützenden Assets auf generischem Level identisch, wenngleich anders gewichtet.

Im September 2021 hat die Bundesregierung die aktualisierte Cybersicherheitsstrategie für Deutschland [7] beschlossen, mit dem Ziel, Cybersicherheit mit einem dem Schutzbedarf der IT-Infrastrukturen angemessenen Level zu begegnen. Eines der Kernelemente ist der Schutz nationaler IT-Systeme in Deutschland, insbesondere im KRITIS-Bereich. Darin wurde bereits die weltraumbasierte Infrastruktur (gemeinsam mit den 5G / 6G-Netzen) als „Rückgrat der Digitalisierung der Gesellschaft" deklariert, welche in einem „ganzheitlichen Ansatz fortlaufend evaluiert und an die neuen Gefährdungen angepasst" werden.

Als Cybersicherheitsbehörde des Bundes sowie als national und international anerkanntes Kompetenzzentrum und Ansprechpartner für Fragen der Informationssicherheit ist das BSI auch für Informationssicherheitsfragen von Satellitensystemen zuständig. Die Grundlage hierfür bildet das BSI-Gesetz [8], welches der Behörde die Aufgabe als zentrale Stelle für Informationssicherheit auf nationaler Ebene zuweist.[6] Nach der BSI-KRITIS-Verordnung [9] ist das BSI zudem für die Informationssicherheit von KRITIS zuständig, zu denen auch die Bodeninfrastruktur von Satellitennavigationssystemen gehört. In diesem Kontext ist zum einen der Gesichtspunkt der Abhängigkeit kritischer Infrastrukturen von Weltraumsystemen zu nennen, wie z.B. Satellitennavigation für Notfall- und Rettungswesen, andererseits wird derzeit geprüft, inwieweit zukünftige Raumfahrtsysteme selbst als kritische Infrastrukturen zu betrachten sind. Im Aufgabenspektrum des BSI ist der Bereich IT-Sicherheit Weltraum insb. für zivil-behördliche und militärische, geheimschutzbetreute Satellitenanwendungen bereits fest verankert, wie z.B. für die Koordinierung / Begleitung der Akkreditierung von Sicherheitsmanagementarchitekturen, das Sicherheitsmanagement für Galileo PRS, die fachliche Unterstützung der Ressorts für militärische und zivil-behördliche Luft- und Raumfahrtanwendungen und die Technische Richtlinie zum Satellitendatensicherheitsgesetz.

Bei der vorliegenden Strategie handelt es sich um eine Strategie des BSI, in der die Rolle, der Anspruch und das Selbstverständnis des BSI im Kontext zahlreicher Stakeholder beschrieben ist. Dabei greift sie die Handlungsfelder und Ziele der nationalen Cybersicherheits-Strategie systematisch auf und schreibt diese für weltraumspezifische Infrastrukturen fort, den aus der Raumfahrtstrategie der Bundesregierung [1] abgeleiteten Empfehlungen und Vorgaben folgend. Die konsolidierten strategischen Ziele, Handlungsfelder und Handlungsziele zur Cybersicherheit Weltraum sind in Kapitel 2 – nach einem Überblick zur Bedrohungslage in Kapitel 1.1 – zu finden. Zweck der Darstellung der Bedrohungslage ist es, die Vielfalt von Bedrohungen für Satellitensysteme aufzuzeigen, sowie zu betonen, dass Bedrohungen allgegenwärtig sind und sowohl klar definiertem Ursprungs als auch undefinierter Natur sein können. Sie bestehen im Cyberraum, im elektromagnetischen Umfeld und im Informationsumfeld. So soll dieser Überblick die Komplexität von Bedrohungen, deren Potenzial und mögliche Konsequenzen veranschaulichen.

In Kapitel 2 werden allgemein gültige Handlungsfelder und Ziele identifiziert. Diese sind nicht notwendigerweise direkt aus den Bedrohungen in Kapitel 1 abgeleitet. Die genaue Zuordnung von Bedrohungen zu Handlungsfeldern und damit entsprechenden Maßnahmen erfolgt unabhängig von dem Strategiepapier im Rahmen einer Risikobewertung und Entwicklung von Mindestanforderungen.

Nächste Schritte, etwa die Planung geeigneter Maßnahmen zur Erreichung der formulierten Handlungsziele und die Erstellung eines Mindestanforderungskatalogs und einer Technischen Richtlinie durch das BSI, werden in Kapitel 3 kurz dargestellt.

1.1 Bedrohungslage

Die Bedrohungen für Satelliten sind mannigfaltig. Wie bereits im vorherigen Abschnitt geschildert, existieren Bedrohungen der Satellitensicherheit[7] unterschiedlichen Ursprungs: diejenigen natürlichen Ursprungs

[6] Im Kontext GALILEO besteht zudem eine Ressortvereinbarung, gemäß derer dem BSI die Aufgabe übertragen wurde, die Ressorts bzgl. IT- und Cybersicherheit von Satellitensystemen zu unterstützen.

[7] Der Begriff Sicherheit unterscheidet im Deutschen nicht zwischen „Safety" und „Security". Im Satellitenumfeld spielt die Security die vorrangige Rolle. Safety ist für die Systeme im Nutzersegment relevant, für

und künstlich herbeigebrachte Bedrohungen, wobei bei Letzteren zwischen nicht vorsätzlichen und vorsätzlichen („Counterspace“ Bedrohungen) unterschieden wird. Abbildung 1 gibt einen Überblick und unterscheidet für die vorsätzliche Bedrohung zwischen vier Counterspace-Technologien:

- EMU[8] physisch – nicht-kinetisch, mit physischer Zerstörung der Betriebsfähigkeit, nicht reversibel
- physisch – kinetisch, mit physischer Zerstörung der Gesamtfunktionalität
- EMU elektronisch, ohne physische Zerstörung der Betriebsfähigkeit, reversibel
- Cyberraum, auf informationstechnisch-logischer Ebene, i.d.R. reversibel

Bedrohungen der Cybersicherheit sind demnach vorwiegend in die vorsätzlich herbeigeführten Bedrohungen einzugruppieren. Neben der in Abbildung 1 dargestellten Kategorie „Cyber“, unter der Bedrohungen wie das klassische Hacken eines Satelliten, Datenabfang und -korrumpierung, Übernahme der Steuerungskontrolle etc. gefasst sind, haben auch die „elektronischen Bedrohungen“ (Spoofing, Jamming, Meaconing) im Cyber-und Informationsraum Relevanz, werden hier aber nicht vertieft.

Im Cyberkontext muss zwischen zwei grundsätzlichen Bedrohungsarten unterschieden werden. Es gibt Bedrohungen, welche die Nutzbarkeit des Gesamtsystems Weltraum (also die terrestrischen, die extraterrestrischen und die elektromagnetischen Anteile) gefährden, und solche, welche innerhalb des Gesamtsystems wirken. Im erstgenannten Szenario ist damit für einen Nutzer von „Weltraumservices“ der Grundwert der Informationssicherheit „Verfügbarkeit“ bedroht, während im zweiten Szenario die Grundwerte „Vertraulichkeit“ und „Integrität“ bedroht werden. Zwar kann davon ausgegangen werden, dass kommerzielle Anbieter von Weltraumdienstleistungen ein intrinsisches Interesse daran haben, ihre Dienstleistungen entsprechend den Kundenanforderungen (und damit des Marktpotenzials) informationssicher anzubieten, doch kann aufgrund von entsprechenden Umständen (bspw. Gesetzeslage, unterschwellige Beeinflussung etc.) in einigen Weltraumnationen eine nachrichtendienstliche „Mitnutzung“ der Weltraumdienstleistungen nicht immer ausgeschlossen werden. Daher ist bei Nutzung von gewerblichen Weltraumdienstleistungen auch immer die jeweilige Situation im Ursprungsland bezüglich dessen Interessen in Bezug auf und dessen Beziehungen zur Bundesrepublik Deutschland in der Entscheidung zur Nutzung mit zu berücksichtigen. Dies betrifft nicht nur staatliche Akteure, sondern auch privatwirtschaftliche. Vor dem Hintergrund zukünftiger Trends zur Weltraumnutzung ist davon auszugehen, dass Informationsgüter der deutschen Wirtschaft weiterhin von hohem Interesse für fremde Mächte / Volkswirtschaften sind.

Bei einer Betrachtung der wichtigsten Cyberbedrohungen für Satellitensysteme wird auf generischem Level nicht zwischen verschiedenen Satellitenanwendungen unterschieden – trotz der vielfältigen Anwendungen, die sich auf Missionsebene stark unterscheiden, sind die Bedrohungen im Cyberkontext die gleichen. Insbesondere greifen für alle Weltrauminfrastrukturen zunächst die terrestrischen Bedrohungen / Gefährdungen, wie im BSI-IT-Grundschutz-Kompendium [10] in der aktuellsten Version bzw. ISO 27005 oder vergleichbaren Standards aufgeführt. Der Großteil der in [10] gelisteten elementaren Gefährdungen ist trivial abbildbar, beispielsweise ist die Gefährdung G 0.1 des IT-Grundschutzkompendiums, „Feuer“, für einen Hersteller stets ernst zu nehmen, ob es sich um die Herstellung von Satelliten oder Zügen handelt. Einige der Gefährdungen aus [10] erfahren bei Detaillierung möglicher Szenarien und Bewertung im Rahmen einer Risikoanalyse besondere raumfahrtspezifische Relevanz. Als Beispiel sei die Gefährdung G 0.12 des IT-Grundschutz-Kompendiums, „elektromagnetische Störstrahlung“, genannt, welche im Zusammenhang mit Satelliten die Bedrohung Jamming des Satellitensignals beinhaltet.

Neben solchen direkten Angriffsszenarien ist mit einem Blick auf die Entwicklung der Satellitensysteme von Beginn bis heute (und einer Prognose für zukünftige Systeme) ein nicht zu vernachlässigendes Gefahrenpotential erkennbar: während die frühen Satelliten vorwiegend große, langlebige, wertvolle Einzelstücke

die Satelliten-systeme selbst ist sie nachrangig. Cybersicherheit ist ein Aspekt der Security und IT-Sicherheit wiederum ist als Teil der Cybersicherheit zu verstehen. Für die Bedrohungen wird zunächst die Gesamtsicherheit eines Satelliten betrachtet und kategorisiert, um die Untermenge derjenigen Bedrohungen, die die Cybersicherheit betreffen, zu identifizieren.

[8] EMU = elektromagnetisches Umfeld

sind, geht der Trend immer mehr zur Massenproduktion. Gerade für den Einsatz im erdnahen Low-Earth-Orbit (LEO) und Very-Low-Earth-Orbit (VLEO) werden Megakonstellationen aus tausenden Kleinstsatelliten konzipiert, die schnell und günstig produziert werden. Dies birgt selbst ohne ein mögliches Versagen der Technik oder Angriffe auf die IT-Systeme der Satelliten das Risiko von Kollisionen. Die Anzahl an kooperativen und unkooperativen Objekten nimmt stetig zu, ohne ein verbindliches Space Traffic Management. Dies wird zu vermehrten Kollisionswarnungen führen und den Koordinierungsaufwand erschweren.

Um eine kostengünstige Produktion zu ermöglichen, können Testprozeduren komprimiert werden. Der Wert solcher Satelliten bzw. die Bedeutung auf Missionsebene rechtfertigt aus kommerzieller Sicht nicht den Einbau dedizierter Hardware-Sicherheitsmodule. Das Risiko eines Angriffs auf den nicht cybersicheren Satelliten, so dass dieser durch den Angreifer übernommen, abgeschaltet oder zweckentfremdet wird, nehmen die Unternehmen bewusst in Kauf. Hier ist bis dato ein Defizit an rechtlichen Regelungen für Cybersicherheit von rein kommerziellen Satelliten festzustellen.

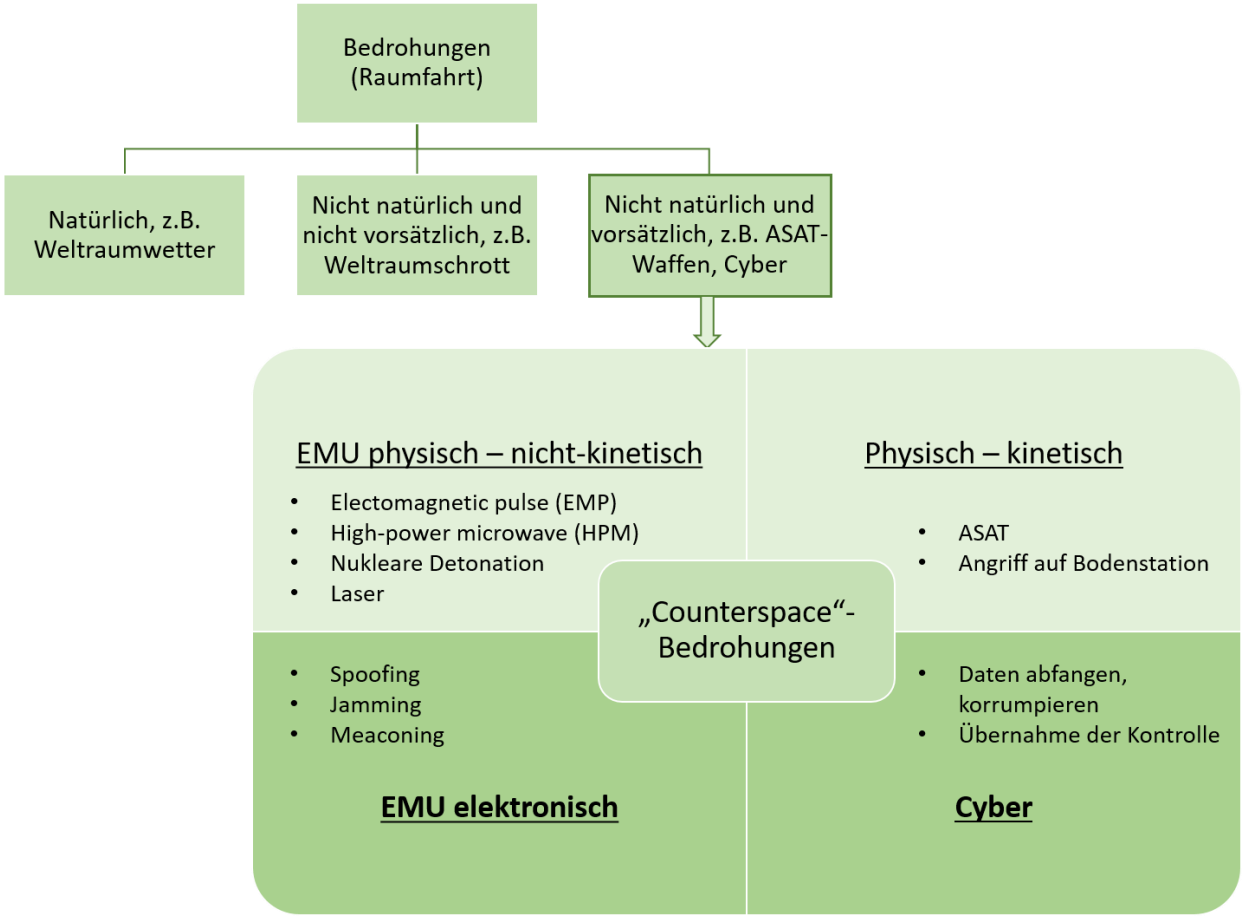

Abbildung 1: Kategorisierung der Bedrohungen in der Raumfahrt und Abgrenzung der Cyberbedrohungen

2 Handlungsfelder und -ziele

2.1 Vorgehensweise

In diesem Kapitel werden die relevanten Handlungsfelder für die Cybersicherheit mit Raumfahrtbezug und dazugehörige Handlungsziele identifiziert. Das Vorgehen zur Ableitung der Handlungsfelder ist schematisch in Abbildung 2 dargestellt: Im ersten Schritt wurden mögliche Handlungsfelder zweigleisig erarbeitet, einerseits auf direktem Weg durch Ableitung aus den Leitzielen / übergeordneten strategischen Zielen für raumfahrtspezifische Cybersicherheit, und andererseits durch Ableitung aus den existierenden nationalen Strategiepapieren zur Cybersicherheit und Raumfahrt.

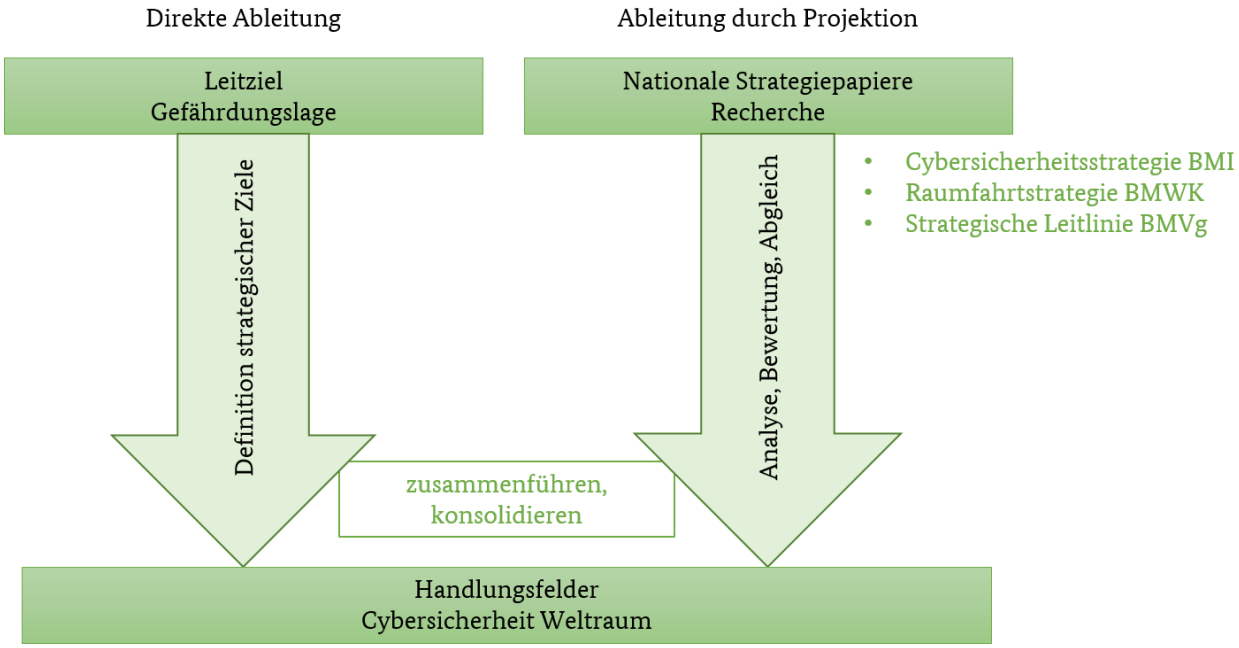

Abbildung 2: Prozess zur Ableitung der relevanten Handlungsfelder für die raumfahrtspezifische Cybersicherheit

Der direkte Weg erfolgte im Rahmen des in Abbildung 3 dargestellten Zielfindungsprozesses, in dem systematisch Ziele aus übergeordneten Zielebenen abgeleitet werden und somit schrittweise konkretisiert werden. Mit dem Fokus auf Cybersicherheit für Raumfahrtanwendungen wurde das in Kapitel 1 vorgestellte übergeordnete Leitziel herunter gebrochen auf strategische Ziele, welche als Basis zur Definition der Handlungsfelder dienen.

Zur Ableitung aus existierenden Strategiepapieren wurden die Handlungsfelder der Cybersicherheitsstrategie

a. Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

b. Gemeinsamer Auftrag Cybersicherheit von Staat und Wirtschaft

c. Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur

d. Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik

auf die Thematik Weltraum projiziert. Für die Analyse und Bewertung jedes Handlungsfeldes wurde sowohl die Relevanz für als auch eine mögliche Sonderstellung eines Cybersicherheitsthemas aufgrund von Weltrauminfrastrukturen untersucht. Ferner wurden mögliche Anknüpfungspunkte zur Cybersicherheit bei den

Handlungsfeldern der Raumfahrtstrategie betrachtet. Anhand der Analyse und Bewertung der zugehörigen Handlungsziele wurde dann entschieden, ob das untersuchte Handlungsfeld im Cyber-Weltraum-Kontext eine zentrale Bedeutung hat, ggf. umdefiniert werden muss oder gänzlich verworfen werden kann. Weitere nationale Strategie-Papiere im Cyber- oder Raumfahrtkontext flossen in einem anschließenden Abgleich ein.

Schließlich wurden die im ersten Schritt direkt und die durch Projektion abgeleiteten Handlungsfelder zusammengeführt, dabei hinsichtlich auftretender Überschneidungen und Lücken geprüft und entsprechend angepasst, um auf die in Kapitel 2.1 vorgestellten zentralen Handlungsfelder zu priorisieren. Aus den so definierten Handlungsfeldern ergeben sich gemäß Abbildung 3 konkrete Handlungsziele, welche in Kapitel 2.2 dargelegt sind.

Durch den vorgestellten querschnittlichen Ansatz aus direkter, an den Leitzielen orientierter Definition der Handlungsfelder und Ableitung aus gegenseitiger Projektion Cybersicherheit und Raumfahrt soll gewährleistet werden, dass die ausgewählten Handlungsfelder ein tragfähiges Gesamtbild ergeben, das vollständig in einem ressortübergreifend akzeptierten Definitionsbereich ist.

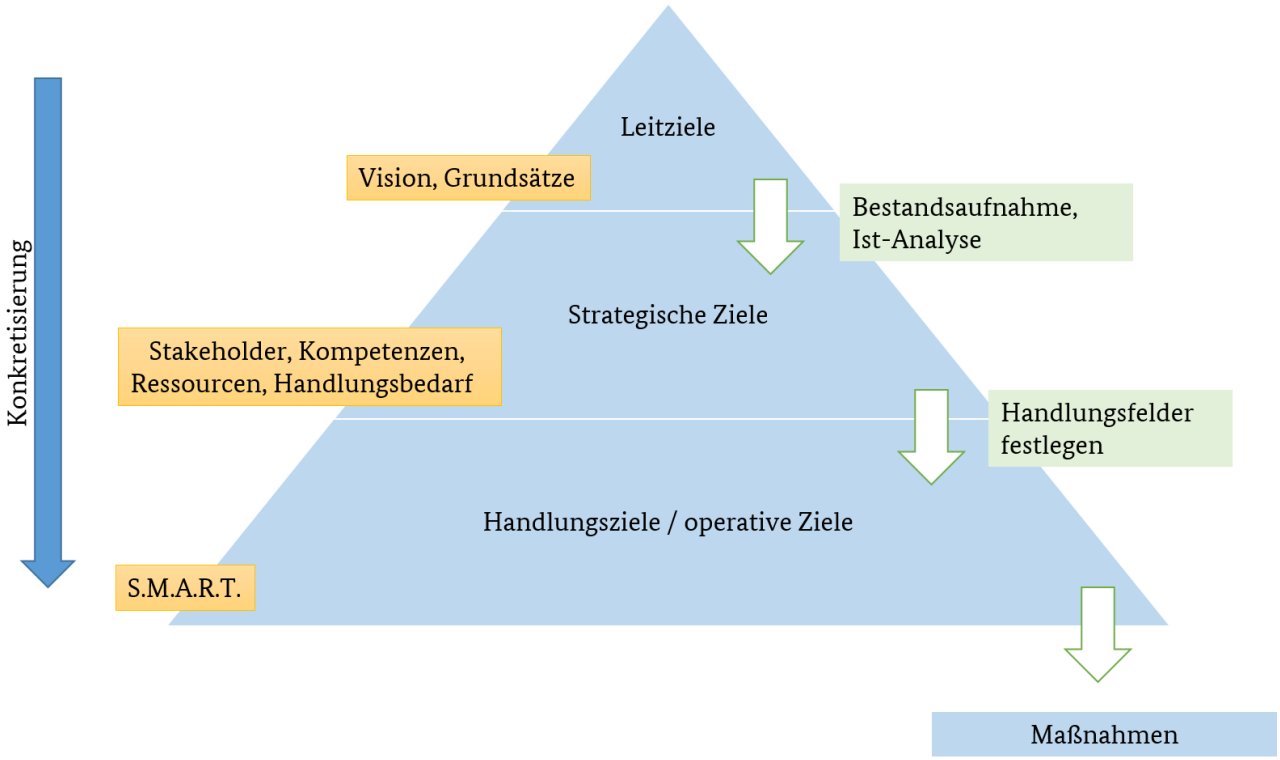

Abbildung 3: Zielfindungsprozess mit verschiedenen Zielebenen: übergeordnete Leitziele (generisch), strategische Ziele (aus welchen sich die Handlungsfelder ergeben) und Handlungsziele (konkret) [11]. Aus Letzteren lassen sich die erforderlichen Maßnahmen zur Erreichung der Handlungsziele ableiten, welche in einem an die Strategie anknüpfenden Dokument behandelt werden.

2.2 Handlungsfelder

Bei der direkten Ableitung der Handlungsfelder werden, wie oben beschrieben, gemäß des in Abbildung 3 schematisch dargestellten Zielfindungsprozesses die Handlungsfelder anhand der strategischen Ziele definiert. An dem in Kapitel 1 eingeführten Leitziel

„Stärkung der Cybersicherheit von Weltrauminfrastrukturen, welche von Relevanz für Staat, Wirtschaft und Gesellschaft sind, zur Sicherstellung der Verfügbarkeit von Diensten über integre, authentische Kommunikation."

orientieren sich vier strategische Ziele, denen wiederum jeweils ein Handlungsfeld zugeordnet wird. Die strategischen Ziele sind in Abbildung 4 aufgeführt.

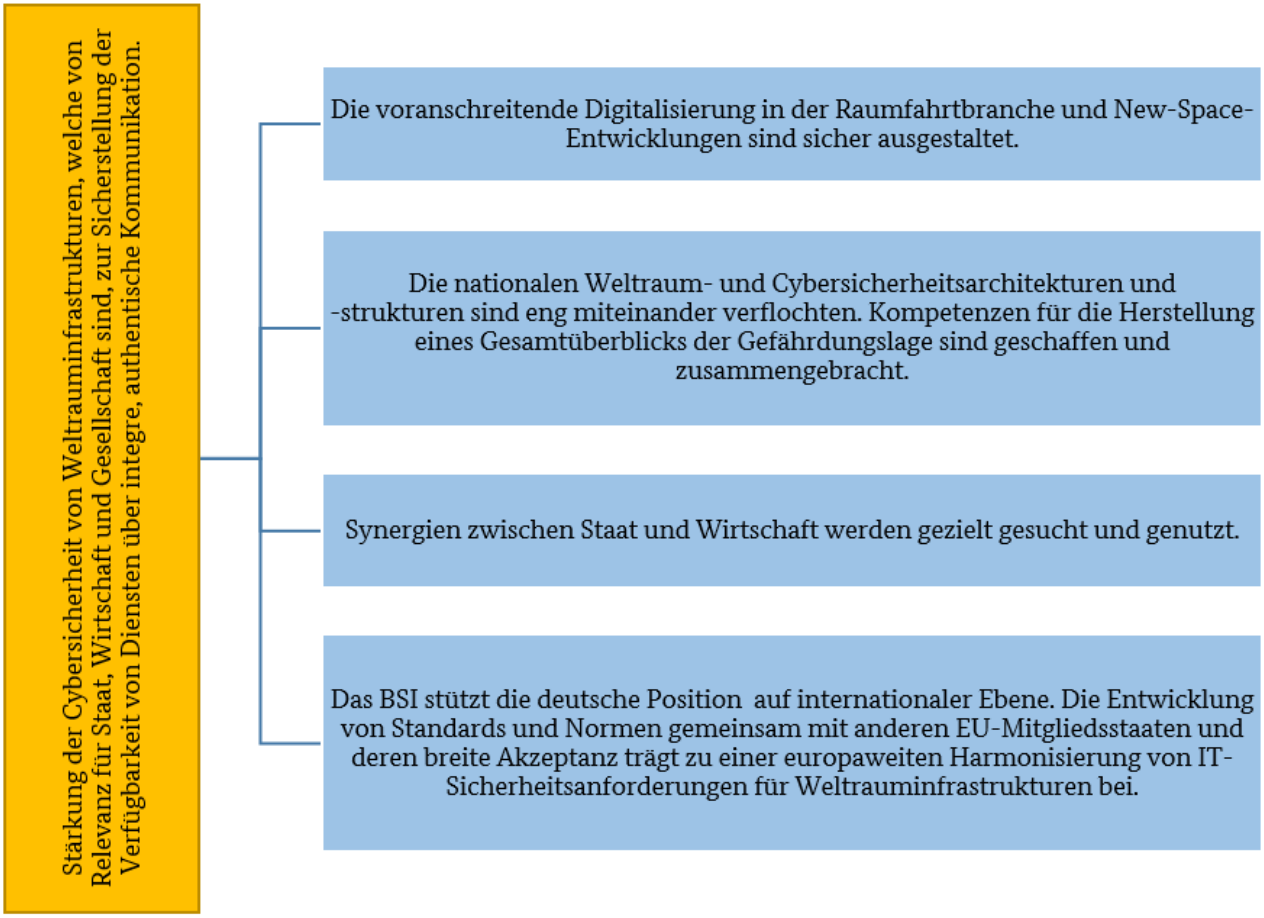

Abbildung 4: Aus dem Leitziel (orange hinterlegt) können vier strategische Ziele (blau hinterlegt) abgeleitet werden.

Die zugeordneten, von der Cybersicherheitsstrategie für Deutschland [7] projizierten Handlungsfelder lauten

i. Sichere Ausgestaltung der New-Space-Ära und Digitalisierung in der Raumfahrtbranche
ii. Zusammenwirken der nationalen Weltraum- und Cybersicherheitsarchitekturen und -strukturen, dabei Schaffung und Zusammenbringen von Kompetenzen für die Herstellung eines Gesamtüberblicks der Gefährdungslage
iii. Ausnutzung von Synergien zwischen Staat und Wirtschaft sowie Bürger und Gesellschaft
iv. Starke Positionierung Deutschlands auf internationaler Ebene und Beitragen zur internationalen Zusammenarbeit / Beziehungen / Austausch, sowie europaweite Harmonisierung von IT-Sicherheitsanforderungen durch Standards und Normen

2.2.1 Handlungsziele

Jedem der identifizierten Strategischen Ziele sind im Folgenden mehrere konkrete Handlungsziele zugeordnet, an denen das BSI eine aktiv gestaltende Rolle übernimmt.

i Die voranschreitende Digitalisierung in der Raumfahrtbranche und New-Space-Entwicklungen sind sicher ausgestaltet.

- Zur Umsetzung von für die Erreichung der Handlungsziele geeigneten Maßnahmen ist 2023 das Schwerpunktreferat für Informationssicherheit im Weltraum im BSI eingerichtet und in der nationalen Weltraum- und Cybersicherheitsarchitektur etabliert und anerkannt.
- Es ist ein umfassendes Wissens-Niveau im Bereich der Weltraum-Cybersicherheit im BSI gewährleistet.
- 2022 sind Mindestanforderungen zu Weltraum-Cybersicherheit identifiziert und in einem Katalog zusammengefasst, 2023 werden diese in einer Technischen Richtlinie detailliert abgebildet.
- Sicherheitsanforderungen werden bereits in der Entwicklungsphase berücksichtigt; bei sicherheitskritischen Missionen erbringen Unternehmen hierzu entsprechende Nachweise (Security-by-Design).
- Hersteller und Betreiber von Satellitenanwendungen wenden einheitliche, auf Raumfahrt zugeschnittene Cybersicherheits-Standards an.
- Die IT-Sicherheitsarchitekturen von Satelliten, die selbst als Verschlusssache (VS) eingestuft sind oder VS-Informationen verarbeiten, basieren auf dem aktuellen technischen Entwicklungsstand und sind durch zulassungsfähige IT-Sicherheitsfunktionen (z.B. Kryptosysteme) geschützt.
- Allen sicherheitskritischen Raumfahrtprojekten liegt ein risikoorientiertes ISMS (Information Security Management System) zugrunde. Dieses basiert auf BSI-IT-Grundschutz, ISO 27001/2. Alternativ kann auch ein mindestens gleichwertiger internationaler Standard (bspw. ISO 2700 X-Familie) herangezogen werden.
- Die Sensibilisierung bzgl. Cyberbedrohungen und das Schaffen eines Sicherheitsbewusstseins bei Bedarfsträgern, Herstellern, Entwicklern und Betreibern von Satellitenanwendungen und -systemen wird aktiv gefördert.

ii Die nationalen Weltraum- und Cybersicherheitsarchitekturen und -strukturen sind eng miteinander verflochten. Kompetenzen für die Herstellung eines Gesamtüberblicks der Gefährdungslage sind geschaffen und zusammengebracht.

- Es bestehen übergreifende Kooperationen, die gezielt zur Thematik der Cybersicherheit im Weltraum in regelmäßigen Arbeitskreisen zusammentreffen. 2022 haben hierzu Auftaktveranstaltungen stattgefunden, es wurden Synergien gefunden und gemeinsame Aktivitäten sind in Planung.
- Durch die nationale und internationale Vernetzung mit Cyber- und Weltraumlagezentren, funktionierender Prozesse zur Informationsweitergabe und Meldepflichten bei Vorfällen können Änderungen der Bedrohungslage früh erkannt werden und entsprechend Maßnahmen zur Prävention kontinuierlich geplant und eingeführt bzw. fortgeschrieben und zur Reaktion rechtzeitig ergriffen werden.
- Nationale Kompetenzen bei Staat und Wirtschaft ergänzen sich. Ein enger Austausch mit Experten aus Wirtschaft und Behörden bzgl. Cybergefährdungen und -sicherheit ist etabliert.

iii Synergien zwischen Staat und Wirtschaft sowie der Gesellschaft werden gezielt gesucht und genutzt.

- Eine Auswahl der im KRITIS-Umfeld etablierten Prozesse zur Stärkung und Gewährleistung der Cybersicherheit ist – soweit notwendig – bis 2023 für Raumfahrtinfrastrukturen übernommen.
- Das BSI berät im Rahmen der Digitalisierung bei zukünftig geplanten hoheitlichen oder sicherheitskritischen Satellitenanwendungen und -systemen über den gesamten Lebenszyklus hinweg zu sicherheitstechnischen Fragestellungen (im Rahmen seiner Kompetenzen). Unternehmen können hinsichtlich der Umsetzung von Projekten zur Verbesserung der Cybersicherheit bei Raumfahrtanwendungen unterstützt und gefördert werden.

iv Das BSI stützt die deutsche Position auf internationaler Ebene. Die Entwicklung von Standards und Normen gemeinsam mit anderen EU-Mitgliedsstaaten und deren breite Akzeptanz trägt zu einer europaweiten Harmonisierung von IT-Sicherheitsanforderungen für Weltrauminfrastrukturen bei.

- Das BSI unterstützt mit seiner Fachexpertise bei der Teilnahme an internationalen Gremien und Organisationen zur Cybersicherheit im Weltraum. Die Brisanz von Cyberbedrohungen ist in Zusammenarbeit mit anderen nationalen Stakeholdern erfolgreich in bestehenden Weltraumsicherheitsgremien verankert.
- Es bestehen zahlreiche Kooperationen mit Partnernationen (bi- und multilateral), mit denen gemeinsame Leitlinien erarbeitet werden.
- Die national entwickelten Sicherheitsanforderungen sind grenzüberschreitend anerkannt. Die internationalen Weltraum-Cybersicherheits-Standards sind konform mit den national erarbeiteten Anforderungen.
- Empfehlungen (und soweit möglich und notwendig, Vorgaben) sind transparent, konsistent und risikoorientiert, sie basieren auf der Anwendung etablierter Standards.
- Das BSI erarbeitet aus seiner fachlichen Sicht Standardisierungen für den Bereich Weltraum Cybersicherheit. Diese werden im IMA als die strategischen Standardisierungsziele der Bundesregierung eingebracht.
- Basierend auf europäischen Weltraum-Cybersicherheits-Standards wird gemeinsam mit nationalen Partnern (Industrie, Ressorts, Behörden etc.) ein europäischer Regulierungsrahmen erarbeitet.

3 Nächste Schritte

Zur Umsetzung der im Rahmen dieser Strategie definierten Handlungsziele sind geeignete Maßnahmen zu definieren und zu ergreifen. Diese werden in einem ersten Schritt katalogisiert und es ist ein Plan für deren konkrete Umsetzung zu erarbeiten.

Diese Dokumente werden einem regelmäßigen Review-Prozess unterliegen, wie in Abbildung 5 angedeutet. So wird die Strategie selbst anlassbezogen oder regelmäßig einmal im Jahr geprüft und ggf. überarbeitet (Erweiterung und Anpassung der Zielpyramide); Maßnahmen, die dem Erreichen der Handlungsziele dienen, werden kontinuierlich dynamisch im Rahmen eines PDCA-Modells (Plan – Do – Check – Act) kontrolliert und entsprechend der Zielvorgaben angepasst.

Ein zentraler Baustein bei der Umsetzung zahlreicher Maßnahmen und dem oben beschriebenen Review- und Managementprozess zur Überwachung und Koordinierung der Ziele wird das Schwerpunktreferat für Informationssicherheit im Weltraum sein, das 2023 im BSI eingerichtet ist. Um die definierten Maßnahmen nachhaltig und souverän umsetzen zu können, sowie zur Festlegung ggf. notwendiger verbindlicher regulatorischer Maßnahmen, bedarf es mittel- bis langfristig einer gesetzlichen Grundlage, etwa durch ergänzende Regelungen im BSI-Gesetz [8].

Einige Maßnahmen werden bereits umgesetzt. So werden z.B. 2022, federführend durch das BSI, Mindestanforderungen in Form eines IT-Grundschutz-Profils herausgegeben. Im Rahmen dieser Mindestanforderungen werden Empfehlungen ausgesprochen. Die Notwendigkeit, neben den empfehlenden Anforderungen verbindliche Vorgaben zu formulieren, wird erörtert. Falls für notwendig befunden, werden im Anschluss die Möglichkeiten erwogen, über den Weg der europäischen Standardisierung europäisch einheitliche Anforderungen zu gestalten und umzusetzen. Zum Zweck einer weiteren Detaillierung der Mindestanforderungen, welche stark abhängig vom anzunehmenden Schutzbedarf der Satellitenmission sind, wird bis 2023 eine Technische Richtlinie zu Sicheren Weltrauminfrastrukturen durch das BSI erarbeitet.

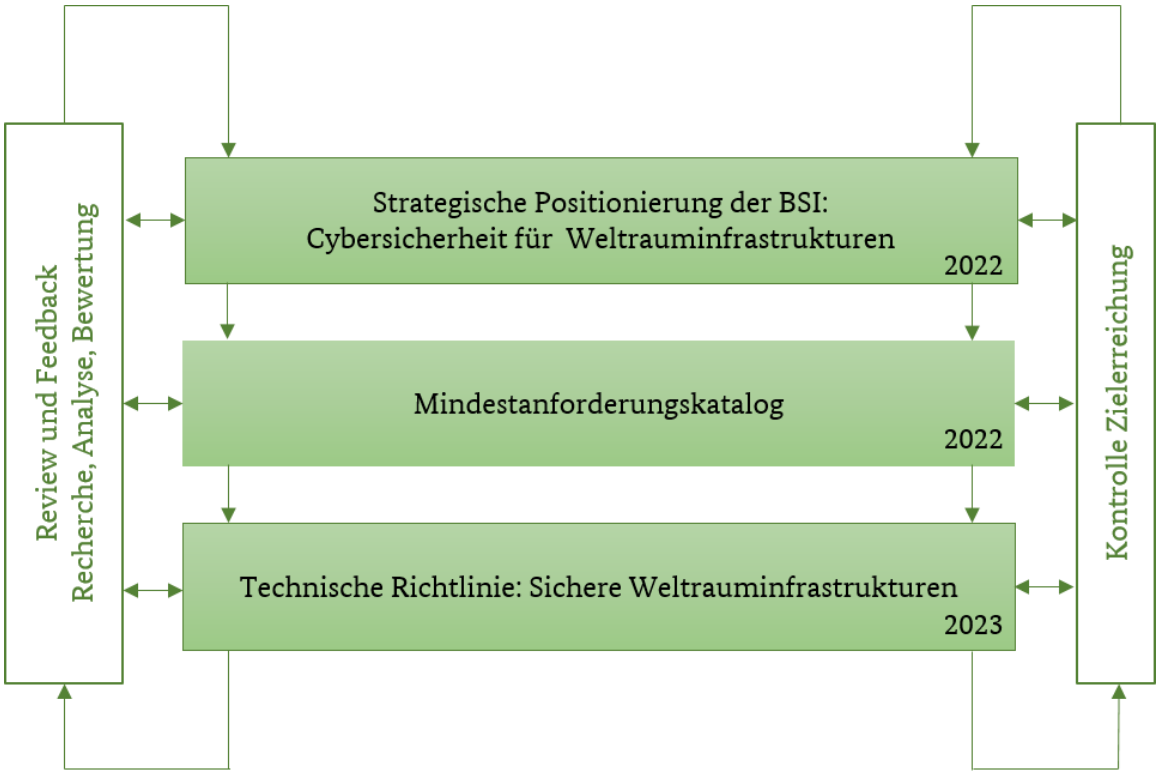

Abbildung 5: Nächste Schritte – im Anschluss an die Strategie werden Mindestanforderungen und eine Technische Richtlinie zu Sicheren Weltrauminfrastrukturen herausgegeben. Die Dokumente sind unter einem ständigen Review-Prozess und werden in regelmäßigen Abständen auf die Erreichung der vorgestellten Ziele überprüft.

4 Glossar

4.1 Begriffsbestimmungen

Bedrohung – Gefährdung:

In der Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Cybersicherheit:

Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyberraum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.

Cybersicherheitsarchitektur:

Die Cybersicherheitsarchitektur eines Landes umfasst alle Akteure – Behörden, Plattformen, Organisationen usw. – die gemäß der nationalen Definition von Cybersicherheit(-spolitik) ein Teil des Ökosystems sind.

Informationssicherheit:

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein.

Informationssicherheits-Management:

Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Informationssicherheits-Management-System (ISMS):

Das ISMS definiert die Methodik, wie das Informationssicherheits-Management umgesetzt wird.

IT-Sicherheit:

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

Jamming:

Jamming bezeichnet das Abstrahlen von Störsignalen, die die ursprünglichen Wellen ganz oder teilweise überlagert. Das Störsignal kann auf der gleichen oder einer benachbarten Frequenz des gestörten Empfängers arbeiten.

Meaconing:

Meaconing basiert wie Spoofing auf der Manipulation gültiger Satellitensignale. Dazu werden Signale empfangen und anschließend wieder ausgesendet. Die ausgesendeten Signale werden also vom Angreifer nicht selbst generiert und weder die Struktur der Signale noch die Spreizkodesequenzen müssen bekannt sein.

Sicherheitskritische Systeme:

Sicherheitskritische Systeme sind Systeme, bei denen Fehler oder Ausfälle bzw. Fehlfunktionen zu ernsthaften Folgen für die menschliche Sicherheit führen kann, z.B. satellitenbasierte Navigationsdienste für die Luftfahrt.

Spoofing:

Im Kontext dieses Dokumentes bezeichnet Spoofing das Täuschen von Satelliten-Signalen durch Aussenden gefälschter, aber gültiger Signale, sodass z.B. im Navigationskontext ein Empfänger falsche Positionsdaten erhält. Im Gegensatz zu Meaconing werden die gefälschten Signale vom Angreifer selbst generiert, der folglich Kenntnis von der Satelliten-Struktur haben muss.

Weltraumsystem:

Oberbegriff für sämtliche Komponenten von Satelliten- und Weltraumlagesystemen. Darunter fallen Weltrauminfrastrukturen selbst sowie die Verfahren zu deren Einsatz, Überwachung, Kontrolle, Betrieb, Nutzung und Schutz.

Weltrauminfrastrukturen:

Unter dem Begriff Weltrauminfrastrukturen werden alle terrestrischen und orbitalen Infrastrukturen (z.B. Satelliten, Kontrollzentren, Bodenstationen) zusammengefasst, die mit den verschiedenen funktionalen Phasen von Weltraumsystemen verbunden sind, wie Betrieb und Nutzung, Kontrolle, Herstellung und Aspekte des Schutzes. Der gesamte Lebenszyklus wird dabei betrachtet.

Literaturverzeichnis

[1] BMWi, „Für eine zukunftsfähige deutsche Raumfahrt - die Raumfahrtstrategie der Bundesregierung," 2010.

[2] BMVg, „Strategische Leitlinie Weltraum," 2017.

[3] G. Falco, *Job One for Space Force: Space Asset Cybersecurity,* 2018.

[4] Chatham House, „Cybersecurity of NATO's Space-based Strategic Assets," The Royal Institute of International Affairs, 2019.

[5] HDI Global Specialty SE, „Satellite Cyberattacks and Security," 2021.

[6] A. Rotter, „Herausforderungen im Weltraum (Arbeitspapier)," BAKS, 2021.

[7] BMI, „Cyber-Sicherheitsstrategie für Deutschland 2021," 2021.

[8] BMJV, „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik," *Bundesgesetzblatt Jahrgang 2009 Teil I Nr. 54,* 2009.

[9] BMJV, „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz," 2016.

[10] BSI, „IT-Grundschutz-Kompendium Edition 2022," 2022.

[11] Beywl, Schepp-Winter (BMFSFJ), „Zielfindung und Zielklärung - ein Leitfaden. Materialien zur Qualitätssicherung in der Kinder- und Jugendhilfe, QS 21," Berlin, 1999.