Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Bern, 25. Oktober 2023

«Cyberrisiken im All»

Bericht des Bundesrates in Erfüllung des Postulats 21.4176 Bellaiche «Cyberrisiken im All» vom 17. Dezember 2021

Inhaltsverzeichnis

Management Summary

Mit der zunehmenden Bedeutung und Nutzung des Weltraums steigen auch die damit verbundenen Abhängigkeiten von weltraumbasierten Anwendungen. Entsprechend haben die direkten und indirekten Verwundbarkeiten durch mögliche Ausfälle weltraumbasierter Dienstleistungen oder gezielte Manipulationen zugenommen. Diese Entwicklungen gehen einher mit der wachsenden Digitalisierung staatlicher und gesellschaftlicher Prozesse. Auch Satelliten sind digitalisiert und softwaregesteuert, was die Angriffsfläche auf das Gesamtsystem dieser Anwendungen vergrössert. Die verstärkte digitale Vernetzung und die Diversifizierung der Akteure und Lieferketten resultieren, wie auch bei terrestrischen Anwendungen, in zunehmend mehr Cyberrisiken. Die Cyberbedrohungslage für terrestrische Anwendungen von böswilligen staatlichen und kriminellen Akteuren gilt in ähnlicher Weise auch für weltraumbasierte Anwendungen. Die kritische Schnittstelle von Weltraum und Cybersicherheit gewinnt in diesem Kontext zunehmend an Bedeutung.

Im Hinblick auf diese Entwicklungen und der aktuellen internationalen sicherheitspolitischen Lage liefert der Bericht eine Bestandesaufnahme der kritischen Abhängigkeiten der sicherheits- und versorgungstechnischen Stabilität der Schweiz von Dienstleistungen und Fähigkeiten der Weltrauminfrastruktur und identifiziert mögliche Massnahmen, um den Handlungsspielraum der Schweiz auszuweiten. Angesichts zunehmender Abhängigkeiten und Verwundbarkeiten kann sich die Schweiz besser schützen, indem sie Redundanzsysteme aufbaut und gezielt eigene Fähigkeiten entwickelt oder nationale Infrastrukturen fördert.

In Verbindung mit der Diversifizierung der Akteure im Raumfahrtbereich und den weltraumbasierten Dienstleistungen sowie technologischen Trends nehmen die Cyberrisiken für die Schweiz zu. Der Bericht legt diese Cyberrisiken für die drei Segmente der Weltrauminfrastruktur «Bodensegment – Datenverbindung – Weltraumsegment» dar. Der Bericht kommt zum Schluss, dass die Schweiz mit einem vergleichsweise kleinen und wenig versorgungs- und sicherheitskritischen Bestand an Weltrauminfrastruktur nur über begrenzte Möglichkeiten verfügt, die Cybersicherheit im Betrieb der Weltrauminfrastruktur auf rein nationaler Ebene zu stärken. Als Forschungs- und Entwicklungsstandort für Technologien, die in Weltrauminfrastrukturen eingesetzt werden, kann die Schweiz jedoch mögliche Massnahmen zur Stärkung der Cybersicherheit in der Entwicklungsphase ergreifen oder sektorspezifische Anreize oder Auflagen für die Entwicklung und Produktion setzen.

Weiter zeigt der Bericht das Schweizer Engagement in multilateralen Gremien, internationalen Organisationen und Entwicklungsprogrammen zu Weltraumthemen und an der Schnittstelle Weltraum-Cybersicherheit auf. Die Schweiz engagiert sich aktiv in verschiedenen UNO-Gremien, sei es in den Bereichen friedliche, sichere und nachhaltige Nutzungen des Weltraums, Weltraumgouvernanz (UNCOPUOS und UNGA), der Koordination der Funknutzung und der Orbitalpositionen aller Satelliten (ITU) oder Meteorologie (WMO) und Weltraumwetter (WMO und UNCOPUOS). Die Schweiz ist Gründungsmitglied von zwischenstaatlichen Organisationen wie der ESA oder EUMETSAT. Sie kann dank der Teilnahme an einzelnen Komponenten des EU-Weltraumprogramms die internationale Raumfahrtinfrastruktursysteme mitgestalten und hat grundsätzlich Zugang zu den für sie wichtigen Infrastrukturen und den daraus abgeleiteten Daten sowie Dienstleistungen. Um ihre Interessen zu wahren, ihren Zugang zum Weltraum zu sichern und ihre Resilienz zu erhöhen sowie ihre Wettbewerbsfähigkeit und Relevanz zu steigern, ist die Schweiz auf die internationale Zusammenarbeit angewiesen. Der Bericht identifiziert mögliche Massnahmen, um den Handlungsspielraum der Schweiz auszuweiten. Konkret bedeutet das, sich weiterhin in internationalen Foren für eine friedliche, sichere und nachhaltige Nutzung des Weltraums einzusetzen und die internationale Zusammenarbeit in der Raumfahrtforschung und -projekten zu intensivieren. Insbesondere sollen die Zusammenarbeit mit der ESA, EUMETSAT sowie der EU im Raumfahrtbereich intensiviert und Synergien mit nationalen Organisationen geschaffen werden sowie der Zugang zu internationalen Beschaffungsverfahren sichergestellt werden.

Schliesslich legt der Bericht die Rechtslage der Datenübermittlung im Weltraum dar. Die Diversifizierung der Akteure im Weltraum nimmt durch den Ausbau kommerzieller weltraumbasierter Dienstleistungen zu. Aus diesem Grund wird die Rechtslage bei der Datenübermittlung im Weltraum komplexer, vergleichbar mit den Entwicklungen im Bereich Recht im Internet oder hinsichtlich der künstlichen Intelligenz. Der rechtliche Rahmen in der Schweiz für die Datenübermittlung im Weltraum ist über das Fernmeldegesetz (FMG) gesetzt. Der Bundesrat hat am 16. Februar 2022 die Ausarbeitung einer Vernehmlassungsvorlage für ein Raumfahrtgesetz in Auftrag gegeben. Auch hier kann der Bund eine mögliche Massnahme ergreifen. Aufgrund der globalen Dimension der Thematik wird die Schweiz die zunehmend geführten juristischen Debatten in internationalen Foren über den rechtlichen Status der im Weltraum übertragenen und gespeicherten Daten im Auge behalten.

1 Einleitung

Weltraumbasierte Anwendungen haben auf vielfältige Weise Einzug in wirtschaftliche, gesellschaftliche und staatliche Prozesse des Alltags gehalten. GPS-Koordinaten und weltraumgestützte Relais sind nicht nur ein wesentlicher Bestandteil der globalen Kommunikationsnetzwerke und der Wettervorhersage, sondern auch von landwirtschaftlichen Betrieben, Stromnetzen, Verkehrsnetzen, Geldautomaten und Digitaluhren. Gleichzeitig hat auch die militärische Nutzung des Weltraums zugenommen und wird sich in den kommenden Jahren rasch weiterentwickeln. Mit zunehmender Bedeutung und Nutzung des Weltraums steigen auch die damit verbundenen Abhängigkeiten. Entsprechend haben die direkten und indirekten Verwundbarkeiten durch mögliche Ausfälle weltraumbasierter Dienstleistungen oder gezielte Manipulationen zugenommen. Bereits ein partieller Ausfall von Satellitendienstleistungen kann überall dort Auswirkungen nach sich ziehen, wo diese Leistungen ohne sichere und genügende Redundanzen zum Einsatz kommen.
Der wachsende Nutzen und die zunehmenden Abhängigkeiten sowie Verwundbarkeiten von weltraumbasierten Anwendungen gehen einher mit der wachsenden Digitalisierung staatlicher und gesellschaftlicher Prozesse. Auch Satelliten sind digitalisiert und softwaregesteuert, was die Angriffsfläche auf das Gesamtsystem dieser Anwendungen vergrössert. Hinzu kommt, dass die Anzahl öffentlicher und privater Akteure, die im Raumfahrtbereich tätig sind, stetig zunimmt. Immer mehr Akteure sind daran beteiligt, satellitengestützte Dienstinfrastrukturen zu entwickeln, herzustellen und zu betreiben. Die verstärkte digitale Vernetzung und die Diversifizierung der Akteure und Lieferketten resultieren, wie auch bei terrestrischen Anwendungen, in zunehmend mehr Cyberrisiken.[1] Die Cyberbedrohungslage für terrestrische Anwendungen von böswilligen staatlichen und kriminellen Akteuren gilt in ähnlicher Weise für weltraumbasierte Anwendungen. Die kritische Schnittstelle von Weltraum und Cybersicherheit gewinnt in diesem Kontext zunehmend an Grösse und Bedeutung.

Der Ukraine-Krieg hat die Kritikalität dieser Schnittstelle bewiesen, sowohl im neuartigen Einsatz von weltraumbasierten Infrastrukturen als Mittel der Kriegsführung, wie auch durch die Verletzlichkeit von Weltraumsystemen und die Erweiterung der Angriffsfläche durch digitale Vernetzung.[2] Das folgende Beispiel zeigt Satelliten als redundantes und zuverlässiges System im Konfliktfall. Russland fügte der ukrainischen terrestrischen Informations- und Kommunikationsstruktur erheblichen Schaden zu, um die Führungskapazitäten der ukrainischen Armee zu schwächen. Durch die Satellitenkonstellation einer US-Firma konnten jedoch nicht nur Mobiltelefonie wieder verwendet, sondern auch speziell leistungsfähige Kanäle für die militärische Nutzung bereitgestellt werden. Die Widerstandsfähigkeit der Satellitenkonstellation verhinderte Versuche Russlands, dieses System zu stören.[3] Zudem konnten die fehlenden oder nicht einsetzbaren luftgestützten Aufklärungs- und Beobachtungsmittel der Ukraine durch Satellitenbilder kompensiert werden, die der Ukraine von verschiedenen unterstützenden kommerziellen Parteien zur Verfügung gestellt wurden.[4] Ein zweites Beispiel des Ukraine-Krieges zeigt im Gegenzug, wie dasselbe vernetzte Weltraumsystem die Angriffsfläche auf Nicht-Konfliktparteien durch Kollateralschäden vergrössern kann. Zu Beginn des Ukraine-Kriegs beeinträchtigte ein Cyberangriff auf die Bodenstation eines kommerziellen Satellitenbetreibers das Kontrollsystem einer kritischen Infrastruktur in Deutschland. Ein Kunde des Satellitenbetreibers, der Windkraftanlagen vor der deutschen Nordseeküste betreibt, steuert seine Windturbinen über Satelliten. Der russische Cyberangriff auf den Satellitenbetreiber beeinträchtigte die Fernsteuerung der Windturbinen temporär.[5] Im Hinblick auf die Ausweitung der Angriffsfläche in Konflikten auf solche kommerziellen Akteure, die weltraumbasierte Dienstleistungen erbringen, können Kollateralschäden häufiger auftreten.[6]
Vorfälle dieser Art sind staats- und sicherheitspolitisch bedenklich und haben Fragen der Sicherheit dieser vernetzten Systeme weltweit in den Fokus gerückt. Auch für die Schweiz existieren Cyberrisiken im

[1] Siehe The Aerospace Corporation, Protecting Space Systems from Cyber Attack, <https://aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368> (besucht am 19. Februar 2023).

[2] Der Schweizerische Bundesrat, Zusatzbericht zum Sicherheitspolitischen Bericht 2021 über die Folgen des Krieges in der Ukraine, 2022, <https://www.vbs.admin.ch/content/vbs-internet/de/home/meta-suche/suche.download/vbs-internet/de/documents/sicherheitspolitik/sicherheitspolitische-berichte/2021/Sicherheitspolitik-Schweiz-Zusatzbericht-Bundesrat-2021.pdf>.

[3] Dieses Beispiel zeigt ausserdem auf, wie ein Staat durch die Nutzung eines privaten Systems auch in eine Abhängigkeit einer privaten Firma gerät, dessen Interessen nicht zwingend deckungsgleich mit der Strategie des Staates sind. <https://www.theguardian.com/world/2023/feb/09/zelenskiy-aide-takes-aim-at-curbs-on-ukraine-use-of-starlink-to-pilot-drones-elon-musk>. (besucht am 10. Januar 2023)

[4] Z. B. Palantirs MetaConstellation, welches direkt Satellitenbilder hunderter Satelliten in die ukrainische Lagebildplattform Delta speist. <https://www.palantir.com/offerings/metaconstellation/> (besucht am 15. Februar 2023).

[5] «Die USA, Grossbritannien und die EU haben diese Cyberangriffe Russland zugeschrieben. (…) Die Angriffe dienten sehr wahrscheinlich dazu, die von der ukrainischen Armee benutzten Kommunikationskanäle zu stören. Sie hatten jedoch Auswirkungen auf mehrere Länder und Kommunikationseinrichtungen ohne Bezug zu den Kriegshandlungen: Unter anderem waren mehrere Windturbinen in Europa betroffen, die danach zwar noch in autonomem Modus Strom produzierten, jedoch nicht mehr aus der Ferne von den Betreiberfirmen überwacht und gesteuert werden konnten.» S. 73-74; Der Schweizerische Bundesrat, Sicherheit Schweiz 2022, 2022, <https://www.newsd.admin.ch/newsd/message/attachments/72368.pdf> (besucht am 12. Januar 2023).

[6] Im September 2022 erklärte der Leiter der russischen Delegation in einer Arbeitsgruppe der Vereinten Nationen (UNO) zu Bedrohungen aus dem Weltraum, dass kommerzielle Satelliten, die zur Unterstützung gegnerischer Streitkräfte eingesetzt werden, ebenfalls "ein legitimes Ziel für Vergeltungsmassnahmen" werden könnten. KATRINA MANSON, The Satellite Hack Everyone is Finally Talking About, Bloomberg, 2023, <https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/#xj4y7vzkg> (besucht am 2. März 2023).

Weltraum aufgrund ihrer Abhängigkeit von Dritten. Der vermehrte Einsatz von Cybermitteln zur Vorbereitung und Unterstützung militärischer Aktionen im internationalen Konfliktfall ist dabei ein Einflussfaktor für die Risikobeurteilung.[7] Neben gezielten und vorsätzlichen Cyberangriffen im militärischen und nichtmilitärischen Kontext ergeben sich Cyberrisiken für die Weltrauminfrastruktur auch aus Naturereignissen und technischen Fehlern.
Aufgrund der Diversifizierung der Akteure sind auch Kleinstaaten mit starken Forschungs- und Entwicklungssektoren in internationalen Foren und Konsortien aktiv und einflussreich. Die Schweiz ist als Forschungs- und Industriestandort mit einer wachsenden Anzahl von Akteuren mit bedeutenden Weltraumaktivitäten in der internationalen Wissensgemeinschaft, in Gremien und Konsortien vertreten.[8]
Im Hinblick auf diese Entwicklungen und der aktuellen internationalen sicherheitspolitischen Lage liefert der vorliegende Bericht eine Bestandesaufnahme für Cyberrisiken in Schweizer Abhängigkeiten von der Weltrauminfrastruktur. Dabei ist wichtig zu unterstreichen, dass Cyberrisiken im Weltraum grundsätzlich durch eine ähnliche Bedrohungslage wie Cyberrisiken terrestrischer Cyberinfrastruktur verursacht werden, d. h. nicht ausschliesslich konfliktbedingt sind. Die Weltrauminfrastruktur ist von staatlichen und kriminellen Akteuren, im Konfliktfall und in Friedenszeiten, während der Herstellung oder des Betriebs angreifbar.
Der Bericht beleuchtet die kritischen Abhängigkeiten der Schweiz von der Weltrauminfrastruktur, die Cyberrisiken, die sich aus diesen Abhängigkeiten ergeben, sowie den internationalen Handlungsspielraum der Schweiz und die Rechtslage der Datenübermittlung.

1.1 Strategische Ausgangslage Schweiz

Cyberrisiken im Weltraum sind ein Thema, welches von mehreren Departementen und Stellen der Bundesverwaltung behandelt wird. Weltraumpolitik und Cybersicherheitspolitik werden Stand 2023 separat behandelt. Für die Schweizer Weltraumpolitik ist der Bundesrat zuständig.[9] Das Staatssekretariat für Bildung, Forschung und Innovation (SBFI) fördert und koordiniert die schweizerischen Aktivitäten zur Erforschung und Nutzung des Weltraums. Verschiedene Departemente und Bundesämter sind in die Erarbeitung und Umsetzung der Schweizer Weltraumpolitik involviert. Effiziente Zusammenarbeit und Koordination wird im Auftrag des Bundesrates vom Interdepartementalen Koordinationsausschuss für Raumfahrtfragen (IKAR) sichergestellt, dessen Vorsitz und Sekretariat durch das SBFI gestellt wird.[10]
Angesichts der Ausweitung der Nutzung von Raumfahrtanwendungen und der Diversifizierung und Zunahme der Akteure, die im Raumfahrtbereich tätig sind hat der Bundesrat beschlossen, die Schweizer Weltraumpolitik von 2008 zu aktualisieren. Die Weltraumpolitik 2023 wurde am 19. April 2023 vom Bundesrat verabschiedet.[11] Sie bildet unter Berücksichtigung verschiedener strategischer Dokumente des Bundesrates den allgemeinen Rahmen für das Weltraummanagement des Bundes.[12] Sie konzentriert sich auf drei strategische Stossrichtungen: (1) Zugang und Resilienz durch gezielte Programmbeteiligungen, Beiträge zur Stärkung der nationalen Handlungsfähigkeit und Einsatz für die nachhaltige und verantwortungsvolle Nutzung des Weltraums, (2) Wettbewerbsfähigkeit und Relevanz durch wissenschaftliche Exzellenz und kompetitive Unternehmen und (3) Partnerschaft und Zuverlässigkeit in der internationalen Zusammenarbeit und gegenüber der schweizerischen Wirtschaft, der Wissenschaft und den Nutzergruppen.
Bezüglich Cyberrisiken im Weltraum verweist die Weltraumpolitik 2023 auf die Verwundbarkeit von Weltrauminfrastruktur und einen Bedarf an Sicherheit und Verteidigung im Sektor im Angesicht der zunehmenden Militarisierung des Weltraums: «Die aufgebauten militärischen Fähigkeiten ermöglichen feindliche Handlungen auf Ziele im All oder auf der Erde, beispielsweise den Abschuss von Satelliten oder Cyberangriffe.»[13] Die Weltraumpolitik verweist auch auf die zunehmenden Abhängigkeiten von Weltrau-

[7] Der Sicherheitspolitische Bericht 2022 des Bundesrates und dessen Zusatzbericht über die Folgen des Krieges in der Ukraine (2022) verweisen auf die zunehmende Bedeutung von Technologiefirmen und deren Zusammenarbeit mit Staaten. Hierzu gehören die erwähnten Hersteller und Betreiber von Weltrauminfrastruktur. Der Schweizerische Bundesrat, Sicherheit Schweiz 2022, 2022, <https://www.newsd.admin.ch/newsd/message/attachments/72368.pdf> (besucht am 12. Januar 2023); Der Schweizerische Bundesrat, Zusatzbericht zum Sicherheitspolitischen Bericht 2021 über die Folgen des Krieges in der Ukraine, 2022, <https://www.vbs.admin.ch/content/vbs-internet/de/home/metasuche/suche.download/vbs-internet/de/documents/sicherheitspolitik/sicherheitspolitische-berichte/2021/Sicherheitspolitik-Schweiz-Zusatzbericht-Bundesrat-2021.pdf>.

[8] z. B. im November 2021, hat das Estländische Wirtschaftsministerium die Cyber and Space Security Conference organisiert und seit 2021 organisiert die ESA zusammen mit CYSEC (EPFL Innovation Park, Lausanne) die Konferenz CYSAT PARIS mit dem derzeit einzigen European satellite hacking challenge. <https://estonia.ee/cssc/>. <https://www.cysec.com/hack-cysat-europes-first-satellite-hack/>.

[9] Dabei stützt der Bundesrat sich zudem auf die Empfehlungen der Eidgenössischen Kommission für Weltraumfragen (EKWF), <https://www.sbfi.admin.ch/sbfi/de/home/forschung-und-innovation/raumfahrt/ekwf.html> (besucht am 6. Juli 2023). Als Kompetenzzentrum des Bundes für nationale und internationale Weltraumfragen fungiert die Abteilung Raumfahrt des Staatssekretariat für Bildung, Forschung und Innovation SBFI, <https://www.sbfi.admin.ch/sbfi/de/home/forschung-und-innovation/raumfahrt/schweizer-weltraumpolitik.html> (besucht am 6. Juli 2023).

[10] Ibid.

[11] Der Schweizerische Bundesrat, Weltraumpolitik 2023, 19. April 2023, <https://www.sbfi.admin.ch/dam/sbfi/de/dokumente/2023/04/publikation_weltraum_politik_2023.pdf.download.pdf/publikation_weltraum_politik_2023_d.pdf>.

[12] Z. B. die Sicherheitspolitischen Berichte 2016 und 2021, die Aussenpolitische Strategie 2020-2023, die Strategie Rüstungskontrolle und Abrüstung 2022-2025 und die Strategie Nachhaltige Entwicklung 2030. Weltraumpolitik 2023, 2023, S. 2.

[13] Weltraumpolitik 2023, 2023, S. 12.

minfrastruktur: «Damit steigt die Verletzlichkeit gegenüber Ausfällen oder Beeinträchtigungen solcher Infrastrukturen. Solche Abhängigkeiten sind besonders dann kritisch, wenn sie die eigene nationale Sicherheit betreffen.»[14] Der Bericht führt diese Abhängigkeiten im Kapitel 2 «Die Abhängigkeiten der Schweiz von der Weltrauminfrastruktur» aus.
Dieser Bericht nimmt die Weltraumpolitik 2023 als eine Grundlage für die Ableitung möglicher Massnahmen für die Minderung von Risiken, die durch Abhängigkeiten von Weltrauminfrastruktur für die Schweiz entstehen. Besonders die erste Stossrichtung «Zugang und Resilienz» leitet Massnahmen für die Schweiz ab, die die Sicherheit der Weltrauminfrastruktur erhöhen sollen. Auch die Massnahmen der Handlungsfelder «Wettbewerbsfähigkeit und Relevanz» und «Partnerschaft und Zuverlässigkeit» gelten grösstenteils auch für die Schnittstelle Weltraum-Cybersicherheit und werden in diesem Bericht entsprechend auf diese Schnittstelle angewandt.
Weitere strategische Dokumente des Bundesrates thematisieren die sicherheits- und versorgungsrelevanten Aspekte der Weltrauminfrastruktur, darunter der Sicherheitspolitische Bericht 2021[15], die Aussenpolitische Strategie 2020-2023[16], die Strategie Digitalaussenpolitik 2021-2024[17] und die Strategie Rüstungskontrolle und Abrüstung 2022-2025[18]. Sie dienen diesem Bericht als zusätzliche Grundlagen für die Ableitung möglicher Massnahmen für die Minderung von Risiken, die durch Abhängigkeiten von Weltrauminfrastruktur für die Schweiz entstehen. Die Cybersicherheitspolitik der Schweiz wird durch das Nationale Zentrum für Cybersicherheit (NCSC) gesteuert. Der Bundesrat hat der Wichtigkeit der Cybersicherheit durch die Überführung des NCSC in ein Bundesamt Rechnung getragen und entschieden, das NCSC ab Januar 2024 beim Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) als Bundesamt anzusiedeln. Das NCSC ist verantwortlich für die Erarbeitung und koordinierte Umsetzung der übergreifenden Nationalen Cyberstrategie (NCS).[19] Die NCS beschreibt die Massnahmen von Bund, Kantonen, Wirtschaft und Hochschulen zur Minderung der bestehenden Cyberrisiken. Sie enthält Massnahmen zur Standardisierung und zur Förderung der Resilienz von kritischen Infrastrukturen gegenüber Cyberrisiken, behandelt jedoch nicht spezifisch Cyberrisiken für Weltrauminfrastruktur. Dieser Bericht nimmt die strategischen Ziele und Grundsätze der NCS als Grundlage für die Ableitung möglicher Massnahmen für den Schutz vor Cyberrisiken, die sich durch die Abhängigkeiten von Weltrauminfrastruktur für die Schweiz ergeben.
Andere Strategien des Bundes verweisen punktuell auf die Schnittstelle Weltraum-Cybersicherheit. Die politische Leitlinie des Bereiches Cyberdefence, die Strategie Cyber VBS, verweist auf bestehendes Potential in der Koordination zwischen den Operationssphären Cyber und Weltraum, spezifisch für die Aufgaben der Armee. Die Strategie Cyber VBS gilt jedoch nicht departementsübergreifend.[20] Cyberrisiken im Weltraum werden auch an der Schnittstelle Bevölkerungsschutz und Cyber adressiert: Die Nationale Strategie zum Schutz kritischer Infrastrukturen 2018 – 2022 (SKI) verweist auf die Verwundbarkeiten von kritischen Infrastrukturen durch den Ausfall weltraumbasierter Dienstleistungen Dritter (z. B. Global Positioning System, GPS oder Galileo).[21]

Vor dieser Ausgangslage beauftragte der Nationalrat mit dem Postulat 21.4176 «Cyberrisiken im All» am 17. Dezember 2021 den Bundesrat, «eine Auslegeordnung über die Situation der Schweiz im Kontext der wachsenden Digitalisierung des Weltraums und die einhergehenden Cyberrisiken zu erstellen sowie daraus erforderliche Massnahmen zu formulieren.» Die Strategien, die die Schnittstelle zwischen Weltraum und Cybersicherheit betreffen, wurden im Jahr 2023 erneuert und in diesen Bericht aufgenommen. Am 5. April 2023 wurde die neue übergreifende NCS vom Bundesrat genehmigt.[22] Die Weltraumpolitik 2023 wurde am 19. April 2023 und die aktualisierte SKI-Strategie am 16. Juni 2023 vom Bundesrat gutgeheissen.[23]

---

[14] Ibid.

[15] Z. B. verweist der Sicherheitspolitische Bericht 2021 des Bundesrates in der Entwicklung des Konfliktbildes auf weltraumgestürzte Aktionen und auf die Wichtigkeit von weltraumbasierten Diensten wie Satellitennavigation oder -kommunikation für Staaten, Wirtschaft und Gesellschaft. Als Massnahmen für die Stärkung der Resilienz und Versorgungssicherheit bei internationalen Krisen werden die Verstärkung des Zugangs zu weltraumbasierten Dienstleistungen zur Kommunikation, Navigation und Erdbeobachtung sowie des internationalen Engagements zur Stärkung der langfristigen und friedlichen Nutzung des Weltraums genannt. Die Sicherheitspolitik der Schweiz Bericht des Bundesrates (2021) BBl 2021 2895, S. 10, 45.

[16] Aussenpolitische Strategie 2020-2023, 2020, <https://www.eda.admin.ch/content/dam/eda/de/documents/publications/SchweizerischeAussenpolitik/Aussenpolitische-Strategie-2020-23_DE.pdf>.

[17] Strategie Digitalaussenpolitik 2021-2024, 2020, <https://www.eda.admin.ch/content/dam/eda/de/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_DE.pdf>.

[18] Strategie Rüstungskontrolle und Abrüstung 2022-2025, 2022, <https://www.eda.admin.ch/content/dam/eda/de/documents/aussenpolitik/strategien/strategie-ruestungskontrolle-und-abruestung-2022-2025-DE.pdf>.

[19] Der Schweizerische Bundesrat, Nationales Zentrum für Cybersicherheit (NCSC), Nationale Cyberstrategie (NCS), 2023, <https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/cyberstrategie-ncs/Nationale-Cyberstrategie-NCS-2023-04-13-DE.pdf.download.pdf/Nationale-Cyberstrategie-NCS-2023-04-13-DE.pdf>.

[20] Die Bundesverwaltung teilt die Verantwortungen in Bezug auf Cyberrisiken in drei Bereiche: Cybersicherheit, Cyberdefence und Cyberstrafverfolgung. Strategie Cyber VBS, 2021, S. 21, <https://www.newsd.admin.ch/newsd/message/attachments/66200.pdf>.

[21] Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022, BBl 2018, 503 ff., S. 513.

[22] Nationale Cyberstrategie NCS, 2023.

[23] Die neue Weltraumpolitik schreibt der kritischen Schnittstelle Cyber und Weltraum mehr Bedeutung zu. Weltraumpolitik 2023, 2023, S. 12, 14; Nationale Strategie zum Schutz kritischer Infrastrukturen, 2023, BBl 2023, 1659 ff..

1.2 Auftrag

Der vorliegende Bericht beantwortet das am 17. Dezember 2021 überwiesene Postulat 21.4176 "Cyberrisiken im All" vom 30. September 2021 von Nationalrätin Judith Bellaiche. Das Postulat lautet wie folgt:

> Der Bundesrat wird gebeten, eine Auslegeordnung über die Situation der Schweiz im Kontext der wachsenden Digitalisierung des Weltraums und die einhergehenden Cyberrisiken zu erstellen sowie daraus erforderliche Massnahmen zu formulieren.

Es wird wie folgt begründet:

> Im Januar 2021 hielt ein Bericht des CSS der ETH Zürich aktuelle Entwicklungen über die zunehmende staatliche und kommerzielle Nutzung des Weltraums für die Übermittlung von Daten fest. In den nächsten Jahren werden zehntausende kommerzielle Kleinsatelliten in den All befördert und Tatsachen in Bezug auf Nutzungshoheit des Weltraums, aber auch Abhängigkeiten schaffen. Die Schweiz verfügt über keinen eigenen Satellitenpark und ist besonders von anderen Staaten und ausländischen Unternehmen abhängig. Daraus ergeben sich Fragen bezüglich der Wahrung der Datensicherheit, sowohl in staatlicher (militärischer) als auch privater Hinsicht.
> Ein Bericht soll aufzeigen, welche Strategie die Schweiz im Kontext dieser Entwicklungen verfolgt und welche Cyberrisiken sich für die Schweiz ergeben - sowohl für den Staat als auch für Private/Unternehmen. Der Bericht soll insbesondere:
>
> - Die Abhängigkeiten der Schweiz von der Weltrauminfrastruktur
> - Die potentiellen Cyberrisiken, die sich daraus ergeben
> - Den Handlungsspielraum und die Einflussnahme der Schweiz innerhalb von Agenturen und Konsortien
> - Die Möglichkeit der Teilnahme an einem Europäische Satellitenkommunikationssystem
> - Die Rechtslage bei der Datenübermittlung im Weltraum
>
> durchleuchten und entsprechende Massnahmen formulieren.

In seiner Stellungnahme vom 24. November 2021 zum Postulat hielt der Bundesrat fest, dass Cyberrisiken im All im Kontext der wachsenden Digitalisierung des Weltraums zu berücksichtigen seien und dass aus Sicht der Cybersicherheit und Cyberdefence nicht nur der Weltraum und Satelliten im Fokus stehen. Vielmehr gehe es darum, das Gesamtsystem für den Betrieb von Satelliten inklusive der terrestrischen Infrastrukturen und Datenflüsse zu betrachten. Dementsprechend sei es angezeigt, sich ganzheitlich mit der Digitalisierung des Weltraums und der damit verbundenen Cyberrisiken zu befassen.

Der vorliegende Bericht zur Erfüllung des Postulats definiert zunächst Schlüsselbegriffe und Konzepte zur Einleitung in die Thematik. Anschliessend werden in den Kapiteln 2-6 die fünf Leitfragen des Postulats nach aktuellem Kenntnisstand beantwortet. In den jeweiligen Fazits werden Schlüsse und mögliche Massnahmen aus den Antworten abgeleitet. Die Leitfrage zum Handlungsspielraum und zur Einflussnahme der Schweiz innerhalb von Agenturen und Konsortien wird begrenzt beantwortet. Der Bund ist als staatliche Instanz nicht in privatwirtschaftlichen Konsortien vertreten, somit sind diese nicht Bestand des Berichtes.
Der Bericht befasst sich mit den für die Schweiz sicherheits- und versorgungsrelevanten Cyberrisiken im Gesamtsystem der Weltrauminfrastruktur. Der Bericht fokussiert dabei auf die Cyberrisiken, die für die zivilen Dienstleistungen und Kompetenzen der Bundesverwaltung und der kritischen Infrastrukturen bestehen. Cyberrisiken bei Dienstleistungen und Infrastrukturen anderer Verwaltungsebenen sind deshalb nicht weniger relevant, werden aber in diesem Rahmen nicht explizit behandelt. Alle Zahlen und Fakten in diesem Bericht basieren auf öffentlich zugänglichen Informationen.

1.3 Begriffserklärung

Nachfolgend werden die für das Verständnis des Berichts zentralen Begriffe und Konzepte erläutert.[24] Des Weiteren wird in die Gesamtstrukturen der Weltrauminfrastruktur eingeführt, diese wird im Bericht nicht technisch detailliert behandelt.

[24] Weitere Fachbegriffe werden im Kapitel 9 «Glossar» beschrieben.

1.3.1 Cyberinfrastruktur, Cyberrisiken und Cybersicherheit

Die Begriffe mit Bezug zu Cyberrisiken werden im vorliegenden Bericht entsprechend der Terminologie der NCS verwendet. Die dort aufgeführten, massgebenden Begriffe sind:

- **Cyberinfrastruktur:** Informations- und Kommunikationsinfrastrukturen (Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln.[25]
- **Cyberrisiko:** Gefahr eines Ereignisses (bemessen durch das Produkt der Eintrittswahrscheinlichkeit und des Schadensausmasses), die dazu führt, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt ist oder es zu Funktionsstörungen kommen kann.[26]
- **Cybersicherheit:** Gesamtheit der Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen und die internationale Zusammenarbeit zu diesem Zweck stärken.[27]

1.3.2 Die Cyberbedrohungslage

Die Cyberbedrohungslage wird von der NCS als der Umstand bezeichnet, der das Potenzial hat, einen Cybervorfall zu verursachen. Die Cyberbedrohungslage hat einen direkten Einfluss auf die Eintrittswahrscheinlichkeit eines Cybervorfalls und somit auf das Gefahrenausmass von Cyberrisiken.
Die NCS unterscheidet zwischen möglichen Cybervorfällen, die durch Cyberangriffe erwirkt werden, und Cybervorfällen, die durch menschliches Fehlverhalten, technische Ausfälle oder technologische Entwicklung ermöglicht werden.
Die Strategie unterscheidet zwischen fünf Arten von Cyberangriffen basierend auf dem Zweck der Angriffe, Akteure, welche hinter den Angriffen stehen, und der Kreis jener, welche angegriffen werden:[28]

- **Cyberkriminalität:** Als cyberkriminell gelten Straftaten, die sich gegen Informations- und Kommunikationstechnik-Infrastrukturen (IKT) richten oder durch IKT ermöglicht werden. Bei Cyberkriminalität steht das Motiv der (monetären) Bereicherung im Vordergrund. Da es nicht das Ziel der Angreifenden ist, das Funktionieren der Gesellschaft, Wirtschaft oder des Staates zu gefährden, beschränken sich die unmittelbaren Auswirkungen oft auf die betroffenen Opfer. Cyberkriminalität ist die Bedrohung mit der höchsten Eintrittswahrscheinlichkeit.
- **Cyberspionage:** Bei der Cyberspionage werden Cyberangriffe dafür eingesetzt, um für politische, militärische oder wirtschaftliche Zwecke unerlaubt an Informationen zu gelangen oder die Aktivitäten der Opfer zu beobachten. Cyberspionage wird von staatlichen ebenso wie von nichtstaatlichen Akteuren ausgeübt. Die Auswirkungen sind meist nicht unmittelbar ersichtlich, da politische und wirtschaftliche Nachteile erst dann entstehen, wenn die Angreifer ihr erlangtes Wissen nutzen. Zudem entstehen im Nachgang solcher Operationen oft enorme Aufwände und Kollateralschäden, da die genutzten Schwachstellen von Cyberkriminellen zweitgenutzt werden.[29]
- **Cybersabotage:** Bei Cybersabotage wird über Cyberangriffe das zuverlässige und fehlerfreie Funktionieren von IKT gestört oder zerstört, was je nach Art der Sabotage und des angegriffenen Ziels auch zu physischen Auswirkungen führen kann.[30] Die Motivation für solche Angriffe kann sehr unterschiedlich sein und Akteure reichen von Einzeltätern, die durch persönliche Frustration getrieben sind, bis hin zu staatlichen Akteuren mit politischen Zielen. Ziel ist in jedem Fall eine Machtdemonstration und Einschüchterung, verbunden mit der Absicht, eine Organisation oder sogar die ganze Gesellschaft zu destabilisieren.
- **Cybersubversion:** Von Cybersubversion wird dann gesprochen, wenn staatliche oder staatsnahe Akteure Cyberangriffe gezielt dafür einsetzen, das politische System eines anderen Staates zu unterminieren. Solche Angriffe zielen beispielsweise auf die Verfahren demokratischer Prozesse (Wahlen und Abstimmungen) ab und werden oft mit Desinformationskampagnen kombiniert.
- **Cyber in militärischen Konflikten:** Der Einsatz von wirtschaftlichen und kriminellen Mitteln in militärischen Konflikten ist heute verbreitete Praxis (hybride Kriegsführung). Cyberangriffe sind

[25] Nationale Cyberstrategie NCS, 2023.

[26] Ibid.; Cyberrisiken nehmen, nicht abschliessend, Form von finanziellen Verlusten, Betriebsunterbrechungen oder eines Schadens durch den Ausfall der Cyberinfrastruktur, die für Informations- und/oder Betriebsfunktionen eingesetzt werden an.

[27] Nationale Cyberstrategie NCS, 2023.

[28] Es ist zu beachten, dass diese fünf Arten häufig in Kombination auftreten und zwischen ihnen Überschneidungen bestehen. Nationale Cyberstrategie NCS, 2023, S. 4.

[29] Mit der Zunahme von geopolitischen Spannungen gewinnt auch die Cyberspionage weiter an Bedeutung. Die Bedrohung wird zusätzlich dadurch erhöht, dass Regierungen Druck auf Hersteller von IKT-Produkten ausüben, damit diese Sicherheitslücken in ihren Produkten offenlassen. Da die Lieferketten bei IKT-Produkten sehr komplex sind und die Schweiz in hohem Mass abhängig von ausländischen Herstellern ist, bleibt Cyberspionage eine zentrale Bedrohung für die Schweiz.

[30] Cybersabotage von kritischen Infrastrukturen kann durch Ausfälle oder Störungen z. B. der Energieversorgung oder Wasserversorgung zu physischen Auswirkungen in Form von Stromausfällen oder Wasserverschmutzung führen.

dabei besonders geeignet, da sie meist nur schwer eindeutig zuzuordnen sind, vergleichsweise wenig kosten, über beliebig grosse Distanzen hinweg einsetzbar sind und es erlauben, politisch-militärische Wirkung in der Grauzone unterhalb der Kriegsschwelle zu erzielen.

Neben gezielten und vorsätzlichen Cyberangriffen können auch unbeabsichtigte Handlungen oder natur- und technikbedingte Ereignisse zu Cybervorfällen führen. Bisher haben Erfahrungen gezeigt, dass hinter vielen grossen Cybervorfällen nicht gezielte Angriffe, sondern Verkettungen verschiedener solcher Umstände wie menschliches Fehlverhalten oder technisches Versagen, verbunden mit einer unzureichenden Vorbereitung, stehen.
Technologische Entwicklungen gelten als zusätzlicher Einflussfaktor auf die Cyberbedrohungslage. Sie können bestehende Bedrohungen verringern, indem sie technische Sicherheit verbessern. Sie erhöhen aber gleichzeitig die Komplexität der Cyberinfrastruktur durch zusätzliche Vernetzung oder führen direkt zu neuen Bedrohungen, indem sie durch Angreifende in Cyberangriffen angewendet werden. Folgende drei Grundlagentechnologien werden durch neue Entwicklungen massgebend die Cyberbedrohungslage beeinflussen: Cloud-Computing, Internet of Things (IoT), Künstliche Intelligenz (KI).[31]

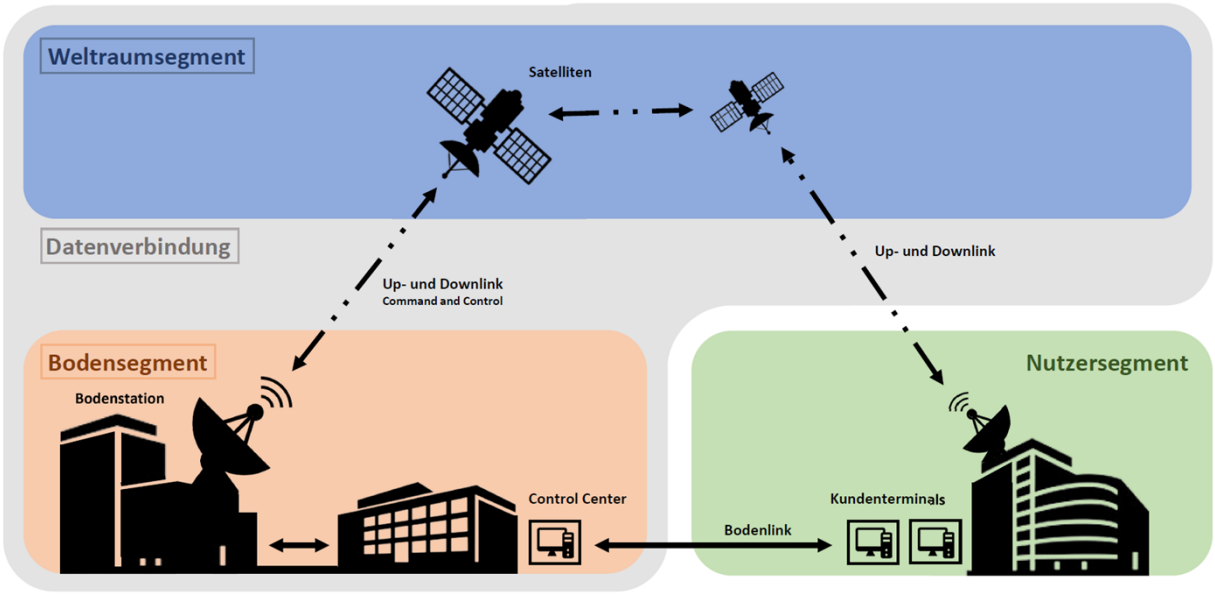
Der vorliegende Bericht geht im Kapitel 3 «Die Cyberrisiken, die sich aus den Abhängigkeiten ergeben» von diesen Phänomenen der Cyberbedrohungslage als grundlegende Einflussfaktoren auf die Ausprägungen von Cyberrisiken aus. Der Bericht skizziert das weltraumspezifische Thema Machine Learning im Weltraum. Andere neue Entwicklungen der Grundlagetechnologien Cloud-Computing, IoT und andere Anwendungen der KI sowie anderer Grundlagetechnologien (z. B. Quantencomputing oder Kryptografie) werden bezüglich neuer Risiken beobachtet. Da sie nicht spezifisch für den Weltraum relevant sind, werden sie in diesem Bericht nicht näher abgehandelt.

1.3.3 Weltraum und Weltrauminfrastruktur

Für den im Postulat genannten Begriff «All» wird der Fachbegriff «Weltraum» verwendet. Eine völkerrechtliche Definition der Abgrenzung dem Weltraum und dem Luftraum, und damit der Abgrenzung der Raumfahrt von der Luftfahrt, gibt es nicht. Sie wurde von der der Fédération Aéronautique Internationale auf eine Grenzhöhe von 100 km (sog. Kármán-Linie) festgelegt als *Raum über dem Luftraum, der rund 100 km über der Erdoberfläche beginnt*. Die US Air Force zieht die Grenze auf einer Höhe von 50 Meilen.

Die Weltrauminfrastruktur besteht aus drei Hauptsegmenten: dem Bodensegment, dem Weltraumsegment und der Datenverbindung dazwischen. Das Nutzersegment ist als angrenzendes Segment zu verstehen und verbindet die Weltrauminfrastruktur mit dem Endnutzer (Abb. 1).[32]

Abb. 1: Weltrauminfrastruktur[33]



[31] Definition Cloud-Computing, Internet of Things, künstliche Intelligenz siehe Glossar. Nationale Cyberstrategie NCS, 2023, S. 7.

[32] Weltraumsysteme umfassen nach Nutzkategorien unterschiedliche Komponente. Für Weltraumaufklärung umfassen sie zusätzlich zur abgebildeten Infrastruktur (Abb 1.) z. B. auch Trägerraketen (Weltraumsegment) und Weltraumbahnhöfe (Bodensegment). Das abgebildete System zeigt die Weltrauminfrastruktur auf, die für die Nutzkategorien der direkten Abhängigkeiten der Schweiz relevant sind (bes. satellitenbasierte Weltraumsysteme).

[33] <https://en.wikipedia.org/wiki/Ground_segment#/media/File:Ground_segment.png>.

Weltraumsegment: Das Weltraumsegment umfasst alle Weltraumgegenstände eines Weltraumsystems. Es besteht z. B. aus einem oder, im Falle einer Konstellation, mehreren Satelliten.

Datenverbindung: Die Datenverbindung bezieht sich auf die Verbindungen zwischen dem Weltraum- und dem Bodensegment, die sogenannten Auf- und Abwärtsverbindungen (Up- und Downlink), sowie Datenverbindungen innerhalb des Weltraumsegments (Satellit zu Satellit).

Bodensegment: Das Bodensegment bezieht sich auf den terrestrischen Teil eines Raumfahrtsystems, der alle Einrichtungen und Elemente umfasst, die für den Betrieb eines Weltraumgegenstandes und die Bereitstellung von Diensten für die Nutzung erforderlich sind. Beispiele für Komponenten des Bodensegments sind Satellitenschüsseln und Empfangsstationen, Operationszentren für die Steuerung, Kapazitäten für die Auswertung von Daten und Antennen für die Datenübertragung.[34]

Nutzersegment: Das Nutzersegment ist die Verbindung zwischen dem Weltraumsegment und den Endnutzern. So bearbeitet es z. B. im Falle einer bildgebenden Dienstleistung die Rohdaten der Kamera eines Weltraumgegenstandes, die über das Bodensegment empfangen werden, um sie für den Endnutzer aufzubereiten und diesem zuzustellen.[35] Die Verbindung zum Endnutzer wird entweder durch eine direkte Datenverbindung zum Weltraumsegment (Up- und Downlink) oder über den Bodenlink zum Bodensegment gestellt.

Weltrauminfrastruktur wird für verschiedene Zwecke eingesetzt. Die Nutzkategorien von Satelliten können in folgenden politischen und rechtlichen Status repräsentiert werden:[36]

Typ	Beschreibung	Beispiele für Dienstleistungen
COM ***Kommerziell***	Gewinnorientierte Nutzung durch einen privaten Akteur	▪ Telefonie ▪ Bildaufnahmen ▪ Breitbandverbindungen
CIV ***Zivil***	Nicht kommerzielle oder staatliche zivile Nutzung	▪ Akademische Projekte ▪ Amateurfunkdienst ▪ Gemeinschaftsinitiativen
GOV ***Staatlich***	Nicht-militärische, staatliche Nutzung	▪ Weltraumaufklärung ▪ Umweltüberwachung ▪ Meteorologie
PPP ***Öffentlich-Private Partnerschaft***	Staatliche und kommerzielle Nutzung	▪ Telekommunikation ▪ Navigation ▪ Bildaufnahmen
MIL ***Verteidigung***	Rein militärische Nutzung / Nachrichtendienst	▪ Militärische Telekommunikation ▪ Frühwarnung ▪ Klassifizierte Bildaufnahmen
DUAL ***Dual***	Militärische und zivile Nutzung	▪ Positionsbestimmung durch Satelliten ▪ Bildaufnahmen ▪ Elektronische Aufklärung

2 Die Abhängigkeiten der Schweiz von der Weltrauminfrastruktur

Die Schweiz ist in zwei Hinsichten von der Weltrauminfrastruktur abhängig: Zum einen in der unmittelbaren Nutzung von Diensten und Anwendungen wie der Navigation, Satellitenkommunikation, Wetter- und Erdbeobachtung sowie der Beobachtung des sogenannten Weltraumwetters. Wenn Behörden und Organisationen der öffentlichen Sicherheit diese Dienste und Anwendungen nutzen, können diese direkten Abhängigkeiten sicherheits- und versorgungsrelevant sein. Zum anderen bestehen indirekte Abhängigkeiten, wenn diese Dienste und Anwendungen in wichtigen Aspekten des täglichen Lebens wie Energieversorgung, Logistik und Verkehr und IKT zum Einsatz kommen. Diese Infrastrukturen werden nach ihrer Kritikalität für das Funktionieren der Wirtschaft und das Wohlergehen der Bevölkerung in Teilsektoren eingestuft. Bei den indirekten Abhängigkeiten konzentriert sich der Postulatsbericht auf jene Teilsektoren kritischer Infrastruktur in der Schweiz, die sowohl eine sehr grosse Kritikalität als auch eine

[34] UN General Assembly, Threats to the security of space activities and systems, 2022, A/AC.294/2022/WP.16, <https://documents.unoda.org/wp-content/uploads/2022/08/20220817_A_AC294_2022_WP16_E_UNIDIR.pdf>.

[35] Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), Reglement 50.041 d, Begriffe Führungsreglemente der Armee 17 (BFA 17), 2018; VBS, EM cdmt Op, Referenzwerte und Kategorien für den Bereich Weltraum, 2021.

[36] Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), Reglement 50.041 d, Begriffe Führungsreglemente der Armee 17 (BFA 17), 2018.

direkte Abhängigkeit von Weltraumsystemen aufweisen. Dies gilt insbesondere für die kritischen Teilsektoren Strassenverkehr, Schienenverkehr, Stromversorgung und Telekommunikation.[37]
Bei der Analyse der indirekten Abhängigkeiten kritischer Infrastrukturen ist die Berücksichtigung sogenannter Kaskadeneffekte entscheidend, d. h. inwieweit der Ausfall einer Infrastruktur zu Ausfällen weiterer Dienstleistungen führt.[38] Das Ausmass von Kaskadeneffekten und deren Verkettung sind beeinflusst durch die Dauer der Störung oder des Ausfalls weltraumbasierter Dienstleistungen und der Bereitstellung von Resilienzmassnahmen. Resilienzmassnahmen können Kaskadeneffekte eindämmen, und spielen eine entscheidende Rolle. Im Bereich der technischen Systeme können dies beispielsweise gezielte Betriebsunterbrechungen sein oder die Abkoppelung von Netzwerkbereichen, um das Ausmass von Kaskadeneffekten einzugrenzen. Der vorliegende Bericht behandelt diese indirekten Abhängigkeiten nicht abschliessend, sondern fokussiert auf jene hoch kritischen Infrastrukturen, deren Ausfall die sicherheits- und versorgungsrelevante Lage der Schweiz unmittelbar beeinträchtigt.[39]
Für die Beschaffung oder Bereitstellung der in diesem Kapitel beschriebenen sicherheits- oder versorgungskritischen Leistungen und Fähigkeiten besteht eine grundsätzliche Abhängigkeit der Schweiz von der Weltrauminfrastruktur. Der Bund und der private Sektor sind für die Herstellung und den Betrieb von Weltrauminfrastruktur, der zugrundeliegenden Cyberinfrastruktur und den Dienstleistungen dieser kritischen Fähigkeiten von Dritten abhängig. In der Schweiz werden einige wenige Satelliten und Bodenstationen betrieben, die meisten von privaten Unternehmen.[40] Das Weltrauminfrastrukturinventar (Bodenstationen) der Schweizer Armee ist für die Auftragserfüllung der Armee geringfügig kritisch.

2.1 Direkte Abhängigkeiten

Positioning, Navigation, Timing (PNT)
Die von öffentlichen und privaten Nutzern am häufigsten in Anspruch genommene Dienstleistung der Weltrauminfrastruktur sind die PNT-Signale (Positioning, Navigation, Timing) der globalen Satellitennavigationssysteme (Global Navigation Satellite System, GNSS). Die satellitengestützte Positionierung und Navigation basieren u. a. auf der Übertragung hochpräziser Zeitangaben. Aus diesem Grund ermöglichen diese Satelliten neben der Herleitung von Positionsinformationen gleichzeitig auch grossräumige Zeitsynchronisationen, z. B. für Energie- und Datenübertragungsnetze sowie für Datenverarbeitungssysteme. Hierfür werden vor allem das amerikanische GPS und bisher in geringerem Umfang das europäische Galileo-System, das russische GLONASS und das chinesische BeiDou-System genutzt.
PNT-Dienste werden vor allem deshalb genutzt, weil sie überall, jederzeit und insbesondere kostenlos verfügbar sind.[41] Darüber hinaus ermöglichen sie, mit einem vergleichsweise geringen technischen Aufwand ein Höchstmass an Präzision zu erreichen. Allerdings besteht bisher keine Garantie für die Verfügbarkeit und Integrität der Signale. Eine Ausnahme wird das PNT-Signal «öffentlich-regulierter Dienst» (Public Regulated Service, PRS) sein, welches die Europäische Union (EU) in ihrem Galileo-Programm aufbaut. Dabei handelt es sich um ein hochverfügbares und verlässliches PNT-Signal, das ausschliesslich staatlich autorisierten Nutzern zugänglich sein wird. Das Kooperationsabkommen zwischen der Schweiz und der EU zur Beteiligung an Galileo und am European Geostationary Navigation Overlay Service (EGNOS) sieht die Möglichkeit vor, dass die Schweiz über ein spezielles Zusatzabkommen den Zugang zum PRS-Signal erlangen könnte. Die EU ist bisher zur Aufnahme von Verhandlungen über dieses Zusatzabkommen mit der Schweiz nicht bereit.
Mit Ausnahme der Nutzung des im Aufbau befindlichen PRS-Signals, dessen Verlässlichkeit und Qualität durch die EU gewährleistet werden wird, obliegt es den Nutzern, die Verfügbarkeit und vor allem die Integrität der PNT-Signale zu überprüfen. In den Organisationen des Bundes, für deren Aufgabenerfül-

[37] Bundesamt für Bevölkerungsschutz BABS, Die kritischen Infrastrukturen, <https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html#ui-collapse-758> (besucht am 20. Januar 2023).

[38] Kaskadeneffekte charakterisieren sich durch eine komplexe und multidimensionale Dynamik, die sich nach einem auslösenden Ereignis über eine kürzere oder längere Zeitdauer in eine Vielzahl unterschiedlicher weiterer Effekte entwickelt. Das erste Ereignis kann geringfügige natürliche, technische oder menschliche Ursachen haben und die Folgeereignisse unterschiedlich starke Disruptionen physischer, gesellschaftlicher, wirtschaftlicher oder auch politischer Art zeitigen. PESCAROLI/ALEXANDER, A definition of cascading disasters and cascading effects: Going beyond the “toppling dominos” metaphor, GRF Davos Planet@Risk, 2015, <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e056c0990d341ce554b98d25d2bca935623ad76>.

[39] Der Bericht befasst sich mit indirekten Abhängigkeiten kritischer Infrastrukturen in der Schweiz, die eine sehr hohe Kritikalität aufweisen. Bundesamt für Bevölkerungsschutz BABS, Die kritischen Infrastrukturen, <https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html#ui-collapse-758> (besucht am 20. Januar 2023).

[40] Gemäss der UCS Satellite Database sind Stand Mai 2022 15 Satelliten In-Orbit in Besitz von Schweizer Akteuren (private Akteure und Hochschulen). UCS Satellite Database, <https://www.ucsusa.org/resources/satellite-database> (besucht am 12. Januar 2023). Vor Inbetriebnahme von Satellitenkonstellationen müssen vorerst Frequenznutzung und Orbitalposition auf internationaler Ebene mit den 193 UNO-Administrationen koordiniert werden. Der Koordinationsprozess kann bis zu sieben Jahre dauern. Stand Mai 2023 befinden sich gemäss der Datenbank der ITU-R ca. 100 Satelliten von Schweizer Betreibern in Koordination. Es ist entsprechend zu erwarten, dass die Zahl der Satelliten schweizerischer Betreiber in den kommenden Jahren deutlich zunehmen wird. BR IFIC (Space services) – Database description, ITU-R, <https://www.itu.int/en/ITU-R/space/Pages/bificDatabase.aspx>.

[41] Die Schweiz bezahlt der EU für Galileo/EGNOS einen jährlichen Beitrag an Aufbau und Betrieb. Deshalb ist Galileo/EGNOS nicht im eigentlichen Sinne kostenlos.

lung PNT-Dienste wichtig sind, ist ein Bewusstsein für diese Verletzlichkeit vorhanden. Die Signalqualitäten werden laufend überprüft.

Weltraumwetterbeobachtung
Die Beobachtung des Weltraumwetters umfasst beispielsweise Sonnenstürme, den Sonnenwind und kosmische Strahlung sowie die Überwachung des Weltraums bezüglich potenziell gefährlicher erdnaher Objekte wie Asteroiden, Meteoriden, auf die Erde abstürzende Satelliten oder Weltraumschrottteile. In diesen Bereichen werden heute überwiegend satellitenbasierte Daten verwendet, entsprechend hoch ist die Abhängigkeit gegenüber Störungen oder Ausfällen.

Wetter- und Erdbeobachtung
Bei der Wetter- und Erdbeobachtung bestehen heute grosse Abhängigkeiten von Daten, die von Satelliten gewonnen und auf die Erde gesendet werden. Der Zugriff auf Daten der Wettersatelliten ist durch die Mitgliedschaft der Schweiz bei der European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT) vertraglich geregelt. Zudem hat der Bundesrat am 16. Februar 2022 entschieden und am 21. Juni 2023 bekräftigt, dass die Schweiz eine Teilnahme am EU-Erdbeobachtungsprogramm Copernicus anstrebt, welches eine breite Palette an Geoinformationen, z. B. im Bereich des Umwelt-Monitorings, anbietet.[42] Die Verwendung von Daten der Erdbeobachtungs- und Wettersatelliten führt aufgrund der internationalen Vernetzung auch zu einer indirekten Nutzung der satellitengestützten Kommunikation. Die Informationen von Wettersatelliten kommen indirekt auch überall dort zum Tragen, wo Meteo-Dienste in Anspruch genommen werden. Dasselbe gilt für Positionierungs- und Navigationsdienste, welche eine wichtige Rolle bei der Herstellung von Geo-Daten spielen, die von vielen öffentlichen und privaten Akteuren genutzt werden. Die satellitengestützte Erdbeobachtung spielt für Behörden der Aussen- und Sicherheitspolitik wie Diplomatie, Nachrichtendienste, Armee, Katastrophen- und Entwicklungshilfe zunehmend eine bedeutende Rolle für die Herstellung von Lagebildern. Datenausfall oder -manipulation können die Lageverfolgung, die Planung und die Führung von Einsätzen einschränken.

Kommunikation und Medien
Satellitentelefone sind bei verschiedenen Krisenorganisationen vorwiegend als Rückfall-Technologie im Einsatz. Auf Stufe Bund ist dies namentlich im Departement für auswärtige Angelegenheiten (EDA), im Justiz- und Polizeidepartement (EJPD) und im VBS der Fall. Der Zugriff auf die Kommunikationsdienste ist in diesen Fällen mit Providern im In- oder Ausland vertraglich geregelt. Diese wiederum stützen sich auf die Dienste ausländischer Satellitenbetreiber. Sollte die Kommunikation über die regulären Netze, im Inland z. B. das Mobilfunknetz, nicht mehr vollständig verfügbar sein, kann auf Satellitentelefonie zurückgegriffen werden. Bei einem gleichzeitigen Ausfall beider Technologien wäre die Einsatzfähigkeit von Krisenorganisationen beeinträchtigt und es entstünde eine sicherheitsrelevante Situation. Ausserhalb des Kreises sicherheitskritischer Behörden und Organisationen verursacht ein Ausfall der Satellitenkommunikation an sich keine versorgungsrelevante Mangellage. Entsprechend gilt die Kommunikation mit Satellitentelefonen gemäss dem Landesversorgungsgesetz nicht als versorgungsrelevanter Service.
Wer Radio- und TV-Signale ausschliesslich über einen persönlichen Parabolspiegel empfängt, kann durch den Ausfall der PNT-Signale beeinträchtigt sein. Auch dieser Service gilt in der Schweiz nicht als versorgungrelevant.

2.2 Indirekte Abhängigkeiten

Energieversorgung
Insbesondere Stromversorgungsnetze nutzen PNT-Signale in ausgeprägter Form. Generell ist die Stromversorgung darauf angewiesen, die Spannung im Netz ausgeglichen zu halten. Je grösser im geografischen und quantitativen Sinn Übertragungs- und Versorgungsnetze sowie ihre Steuersysteme sind, desto kritischer wird die rasche und präzise Steuerbarkeit der Netzspannung, um Ausfälle zu vermeiden. Die Nutzung von PNT-Signalen zur Netzüberwachung ist hierfür beispielhaft und wird entsprechend eingesetzt. Die Stromversorgung ist nicht nur eine kritische Infrastruktur, sondern auch von entscheidender Bedeutung für die Auslösung und Verstärkung von Kaskadeneffekten. Die grossflächige Netzübertragung grosser Strommengen stellt insgesamt eine der kritischsten Abhängigkeiten von Weltrauminfrastrukturen dar. Bei der in der Einleitung erwähnten Störung der Windkraftturbinen in der Nordsee wurde nicht die Nutzung des PNT-Signals gestört, sondern die satellitenbasierte Kommunikation zur Steuerung der Turbinen.

[42] Der Bundesrat, Bundesrat strebt Teilnahme an Copernicus an, 16. Februar 2022, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-87213.html>.

Logistik und Verkehr
Satellitengestützte Navigationssysteme dienen in der Logistik der Effizienzsteigerung. Tourenplanungssysteme können die Positionsdaten von Schiffen oder Lastwagen in Echtzeit überwachen und dadurch die Auslastung sowie die Verkehrslenkung optimieren. Bei einer Störung oder einem Ausfall von Satellitennavigationssystemen können sowohl die Schifffahrt, der Strassenverkehr wie auch die Luftfahrt ihre Versorgungsleistung weiterhin erbringen. Insgesamt ist dabei mit einem Effizienzverlust, nicht aber mit schwerwiegenden Versorgungsstörungen zu rechnen. Je nach Dauer der Störung oder des Ausfalls und der Grösse der betroffenen Fläche können erhebliche negative Auswirkungen auftreten. Ähnlich wie bei der Stromversorgung können auch bei Logistik und Verkehr Kaskadeneffekte eine grosse Rolle spielen.

Telekommunikation und Rundfunk
Neben der direkten Nutzung von Satellitenkommunikation für Telefonie, Radio und TV werden PNT-Signale in der Kommunikation auch indirekt verwendet. Die PNT-Signale werden zur Synchronisierung von Mobiltelefonie-Netzen genutzt. Eine Störung oder ein Ausfall der PNT-Signale würde bedeuten, dass schweizweit Mobiltelefone nur noch beeinträchtigt oder gar nicht mehr genutzt werden könnten, sofern die Anbieter keine geeigneten Massnahmen aktivieren können, mit denen die Netzsynchronisation auch ohne GNSS-Signale sichergestellt werden kann.
Im Bereich des Rundfunks sind Einschränkungen oder Ausfälle von PNT-Signalen kritisch für die terrestrische Verbreitung der digitalen Radioprogramme (T-DAB). Die Infrastruktur von T-DAB basiert auf sogenannten Gleichwellensendernetzen, welche mittels GNSS synchronisiert werden. Wird diese Synchronisation durch ein Ausbleiben der GNSS-Signale beeinträchtigt, so kann dies gebietsweise oder landesweit zu einem Ausfall des Radioempfangs führen. In Notfallsituationen könnte die Bevölkerung somit auch nicht mehr über das Medium Radio informiert werden.

2.3 Beurteilung der Abhängigkeiten

Satellitenbasierte Dienste sind im öffentlichen Sektor punktuell in sicherheitsrelevanten Bereichen, hier vor allem bei der Armee, von Bedeutung. Für öffentliche Stellen ohne unmittelbare Sicherheitsaufgaben sind kaum direkte sicherheitskritische Auswirkungen zu befürchten.
Insgesamt ist die indirekte Abhängigkeit von der Nutzung von PNT-Signalen für die grossflächige Stromversorgung am grössten. In der Mobiltelefonie, in der Verbreitung digitaler Radioprogramme, im Strassenverkehr (Überwachung und Steuerung von Netzen und Signalisationen, vernetztes Fahren, Dienste von Schutz und Rettung), in der Schifffahrt (Positionsbestimmung, Suche und Rettung), im Schienenverkehr (Zugsteuerung und -kontrolle) und in der Luftfahrt (Flug- und Landeprozesse, Überwachung, Suche und Rettung) würden zeitlich beschränkte Ausfälle von PNT-Signalen in erster Linie zu Leistungseinschränkungen führen. Bei länger andauernden und grossflächigen Beeinträchtigungen könnten jedoch Ausfälle zunehmende Auswirkungen haben.
Der wirtschaftliche Schaden bei einem Ausfall der satellitengestützten Meteo-Dienste könnte gravierend sein, da verschiedene Sektoren auf qualitativ hochwertige Wettervorhersagen angewiesen sind (z. B. Energie- und Transportsektor). Ähnliches gilt für die Geo-Dienste. Ein Ausfall hätte mittel- bis langfristig qualitative Auswirkungen auf die räumlichen Planungs- und Führungsgrundlagen auch der Sicherheitsbehörden.
Ein längerfristiger Ausfall von Erdbeobachtungs- und Fernerkundungssatelliten, welche die Erde in verschiedenen Frequenzbereichen beobachten, kann die Forschung, insbesondere in den Klima- und Erdwissenschaften nachhaltig beeinträchtigen. Dies gilt auch für andere Bereiche, welche auf solche Daten angewiesen sind.[43]
Aus den bisherigen Ausführungen kann geschlossen werden, dass Störungen oder ein kompletter Ausfall von PNT-Signalen Kaskadeneffekte auslösen könnten. Hierbei wären in erster Linie die Stromversorgungs- und Strassentransportnetze betroffen, was wiederum Effekte in weiteren Sektoren zur Folge hätte. Es ist jedoch auch darauf hinzuweisen, dass weltraumbasierte Dienste in einigen Bereichen zur Erhöhung der Resilienz von terrestrischen Infrastrukturen beitragen.
Ein Grossteil der satellitenbasierten Dienste kann mittelfristig durch terrestrische oder luftbasierte Systeme ersetzt werden. Dieser Ersatz kann aber die Verfügbarkeit und Effizienz der Dienste teilweise stark einschränken.

2.4 Fazit und mögliche Massnahmen

Verschiedene Sektoren sind von der Weltrauminfrastruktur abhängig. Zukünftig dürfte diese Abhängigkeit der Schweiz grundsätzlich vor allem bei den PNT-Diensten weiter zunehmen. Diese Entwicklung verläuft parallel zur Abhängigkeit von internetgestützten Dienstleistungen in fast allen Lebensbereichen.

[43] Siehe z. B. University of Zurich Department of Geography, Remote Sensing, <https://www.geo.uzh.ch/en/units/rs>.

Der Trend ist einerseits durch die Nutzung der Satellitennavigation und ihre Effizienz zu erklären und andererseits durch die zunehmenden Genauigkeitsanforderungen bei der Zeitsynchronisation terrestrischer Netze, z. B. moderner Kommunikationsnetze wie dem Mobil- und Rundfunk. Unter Umständen können internetbasierte Systeme (NTP oder Radiozeitsignale für Zeit, Geolocation APIs für Positionsdaten)[44] hier eine Alternative bieten, sofern diese Alternativen selbst nicht wiederum satellitenbasierte Systeme als Zweit- oder Hauptquelle für ihre eigenen Zeitsignale nutzen.[45]
Darüber hinaus wird eine starke Zunahme der Abhängigkeit von Erdbeobachtungs- und Meteo-Satelliten erwartet. Unterstützt wird diese Entwicklung durch die zunehmende Kommerzialisierung satellitenbasierter Dienste, welche bis anhin von staatlichen Akteuren mit in der Regel freiem Datenzugang betrieben wurden.
Schwieriger abzuschätzen scheint die Entwicklung im Bereich der autonomen Transportsysteme: Mit zunehmender Nutzung dürfte die Bedeutung satellitengestützter Navigationssysteme steigen und die heutige Beurteilung müsste überprüft werden. Bei autonomen Transportsystemen wird eine Umstellung auf einen Betrieb ohne Personen am Steuer nicht in absehbarer Zeit möglich sein. Zumindest aus heutiger Sicht dient die alternative Positionsbestimmung ohne Satelliten nicht oder nur begrenzt als Ersatz. Gründe hierfür sind z. B., dass eine alleinige Navigation auf Basis alternativer Methoden technisch nicht vorgesehen ist oder dass je nach genutzter Technologie diese nicht überall funktioniert oder genügend genau ist.

Mögliche Massnahmen zur Stärkung der Sicherheit sind in der Weltraumpolitik 2023 angelegt. Einerseits können durch Ausweichlösungen (weltraumgestützt oder terrestrisch) und der Diversifizierung der weltraumbasierten Anwendungen Auswirkungen eines Ausfalls oder einer Störung möglichst klein gehalten werden. Andererseits können durch gezielte Entwicklung eigener Fähigkeiten oder nationaler Infrastrukturen Autonomie und Resilienz erhöht werden. Eigene Fähigkeiten werden insbesondere in den Bereichen Weltraumlageverfolgung (Space Situational Awareness, SSA) und bei der Beurteilung von GNSS-Signalen aufgebaut.[46] Ergänzend zur Beteiligung an internationalen Programmen und nationalen Aktivitäten werden hierfür bi- und multilaterale strategische Partnerschaften geprüft und bei Bedarf ausgebaut.[47]

3 Die Cyberrisiken, die sich aus den Abhängigkeiten ergeben

Die Schweiz ist heute in vielfältiger Weise von Weltrauminfrastrukturen abhängig. Entsprechend sind alle Cyberrisiken, welche die Weltrauminfrastruktur betreffen, für die Schweiz relevant. Cyberrisiken manifestieren sich sowohl bei der Herstellung der für die Weltrauminfrastruktur benötigten Hard- und Software als auch bei deren Betrieb. Cyberrisiken betreffen grundsätzlich alle Teilbereiche der Weltrauminfrastruktur – das Weltraumsegment, das Bodensegment und die Datenverbindung dazwischen. Während die Herstellung und das Bodensegment der Weltrauminfrastruktur ähnliche Cyberrisiken aufweisen wie rein terrestrische Infrastrukturen, gibt es insbesondere beim Weltraumsegment sowie der Datenverbindung einige Risikofaktoren, die hinzukommen oder anders zu beurteilen sind.
Die Ausgestaltung der Weltrauminfrastruktur und ihr Zweck haben einen Einfluss auf die Cyberbedrohungslage, die zu erwartenden Angreifenden, und somit die Ausprägung der Cyberrisiken. Öffentliche oder kommerzielle Satellitennutzung für Erdbeobachtung (z. B. hochaufgelöste Bilder, auf denen kritische Infrastrukturen erkennbar sind) und die Weltraumlage gelten als kritische Dienstleistungen. Die Weltrauminfrastruktur, durch die kritische Leistungen erbracht werden, bietet durch ihren Zweck somit eine Angriffsfläche, um versorgungs- oder sicherheitskritische Effekte zu erzielen. Neben gezielten Cyberangriffen sind auch Cybervorfälle, die durch menschliches Fehlverhalten, technische Ausfälle oder durch technologische Entwicklung ermöglicht werden, Bestandteil der Cyberrisiken der Weltrauminfrastruktur.
Nachfolgend werden einige dieser Risiken für die Herstellung und den Betrieb der Weltrauminfrastruktur sowie für das Weltraumsegment, Bodensegment und die Datenverbindung skizziert. Für eine detailliertere Betrachtung der Cyberrisiken eignen sich z. B. der Bericht zu Sicherheitsbedrohungen für Weltraummissionen vom Consultative Committee for Space Data Systems (CCSDS) oder die Space Attack Research and Tactic Analysis (SPARTA) matrix der Aerospace Corporation.[48]

[44] Definition Network Time Protocol (NTP), Application Programming Interfaces (APIs) siehe Glossar.

[45] Siehe z. B. die GNSS basierte NTP Stratum 1 Infrastruktur der Time Stamping Authority (TSA). Bundesamts für Informatik BIT, TSA-Service, <https://www.bit.admin.ch/bit/de/home/subsites/allgemeines-zur-swiss-government-pki/tsa-service.html#:~:text=Die%20Time%2DStamping%2DAuthority%20(,jeweils%20eingesetzten%20Signatursoftware%20festgelegt%20werden.> (besucht am 12. Januar 2023).

[46] Definition Space Situational Awareness (SSA) siehe Glossar.

[47] Weltraumpolitik 2023, 2023, S. 17.

[48] Das CCDS ist ein multinationales Forum für die Entwicklung von Standards für Kommunikations- und Datensysteme für Weltraummissionen. The Consultative Committee for Space Data Systems, Security Threats Against Space Missions Informational Report, 2022, <https://public.cc-

Gewollte oder ungewollte Fehlleistungen von Satelliten können geschäftsrelevant, respektive sicherheitspolitisch relevant sein. Aus diesem Grund gibt es wenige öffentliche Informationen darüber, in welchem Umfang und mit welcher Häufigkeit welche Ereignisse tatsächlich auftreten. Dies führt dazu, dass die Recherchen nur eingeschränkt möglich sind, was wiederum die vollständige Darstellung der Risiken in diesem Kapitel erschwert.

3.1 Herstellung

Bei der Herstellung von Hard- und Software für Weltrauminfrastruktur können ungewollt oder gewollt Schwachstellen eingebaut werden, welche zu Cyberrisiken für das Funktionieren der Weltrauminfrastruktur werden. Diese Risiken unterscheiden sich grundsätzlich nicht von denen bei der Produktion von Komponenten für andere cybergestützte Infrastrukturen. Sie beinhalten beispielsweise den Einbau von Hintertüren, welche ein privilegiertes Eindringen in ein System ermöglichen. Handelt es sich bei den Hard- und Softwarekomponenten jedoch nicht um Standardkomponenten, sondern um Komponenten, die spezifisch für Weltrauminfrastrukturen gebaut werden, konzentriert sich die Produktion auf einige wenige Hersteller. Dies erhöht die Abhängigkeit von diesen Herstellern und minimiert die Einflussmöglichkeiten die Komponenten möglichst sicher zu gestalten. Darüber hinaus kann auch die Verwendung von gebrauchten oder nicht originalen elektronischen Bauteilen zur Kosteneinsparung problematisch sein. Im Weltraumsegment ist ein Fehlverhalten oder Ausfall einer elektronischen Komponente typischerweise gleichbedeutend mit dem Verlust des jeweiligen Systems. Eine Reparatur oder ein Austausch der defekten Komponente ist kaum möglich. Bei Low Earth Orbit (LEO)-Satelliten wird dieses Risiko etwas entschärft, da diese in der Regel ohnehin eine kurze Lebensdauer haben.

3.2 Betrieb

Der Betrieb des Systems umfasst das Bodensegment, die Datenverbindung und das Weltraumsegment. Analog zur Herstellung entsprechen die Cyberrisiken auch beim Betrieb der Systeme grundsätzlich den Cyberrisiken einer rein terrestrischen Infrastruktur. Abweichungen respektive zentrale zusätzliche Risiken sind nachfolgend für das Bodensegment, das Weltraumsegment und die Datenverbindung aufgeführt.

3.2.1 Bodensegment

Grundsätzlich ist das Bodensegment denselben Cyberrisiken ausgesetzt wie andere terrestrische kritische Infrastrukturen. Die Infrastruktur, die Hardware, die Software und der Datenfluss können beeinflusst werden und können so die Dienstleistung stören, manipulieren oder verhindern.[49] Der Zugriff über die Datenverbindung zum Weltraumsegment bietet Angreifern jedoch zusätzliche kritische Angriffsmöglichkeiten.
Beim Umgang mit Cyberrisiken helfen Cybersecurity Frameworks, wie das des National Institute of Standards and Technology (NIST). Darin wird unter anderem eine Auswahl von Massnahmen definiert, um Cyberrisiken zu mindern. Beispiele für solche Massnahmen sind das zeitnahe Einspielen von sicherheitsrelevanten Patches, Updates und Upgrades, die von den Herstellern zur Verfügung gestellt werden oder sogenannte Penetrationstests, bei denen Fachpersonen beauftragt werden, die Infrastruktur anzugreifen und dabei Schwächen aufzudecken.[50]
Ursprünglich für kritische Infrastrukturen gedacht, findet das NIST-Framework heute auch in der Privatwirtschaft breite Anwendung. Dem Umstand, dass Risiken und Massnahmen je nach Sektor, Zweck und Arten der Infrastruktur anders ausgestaltet sind, wird das NIST-Framework gerecht, indem entsprechende Anwendungsleitfäden zur Verfügung gestellt werden. Dies gibt es auch für das Bodensegment von Weltrauminfrastrukturen.[51]

3.2.2 Weltraumsegment

Das Weltraumsegment ist Einflüssen von Naturereignissen (z. B. Wetterereignisse im Weltraum wie Sonnenstürme, allgemeine Strahlung) oder technischer Art (z. B. Zusammenstösse von Satelliten mit

sds.org/Pubs/350x1g3.pdf>; Space Attack Research & Tactic Analysis (SPARTA), The Aerospace Corporation, <https://sparta.aerospace.org/>.

[49] «Infrastruktur» bedeutet hier die äussere Umgebung z. B. Immobilien. Die «Hardware» ist die materielle Komponente der zu nutzenden IT.

[50] Definition Patches, Updates, Upgrades, Penetrationstest siehe Glossar.

[51] NIST Computer Security Resource Center, NISTIR 8401, Satellite Ground Segment: Applying the Cybersecurity Framework, 2022, <https://csrc.nist.gov/publications/detail/nistir/8401/final>.

anderen Objekten im Weltraum wie Weltraumschrott) ausgesetzt.[52] Bei Naturereignissen bergen besonders Sonnenstürme grosse Cyberrisiken für die Weltrauminfrastruktur. Sonnenstürme können durch Ausstösse elektromagnetischer Strahlung Weltrauminfrastrukturen physisch beschädigen und somit zu Cybervorfällen in Form von Ausfällen von Cyberinfrastruktur kritischer Dienstleistungen führen, wie z. B. Hochfrequenz-Radiokommunikation oder GPS.[53]

Als Einflüsse technischer Art sind gezielte Cyberangriffe auf Satelliten möglich. Angriffe auf Satelliten mit Cyberinfrastruktur können vorübergehend grosse Auswirkungen haben, sind aber oft reversibel. Wenn jedoch ein Angriff das Kommando- und Kontrollsystem eines Satelliten betrifft, kann der Satellit irreversibel funktionsunfähig gemacht werden. Die Kontrolle über den Satelliten selbst kann physisch oder digital übernommen werden, wodurch der Satellit unter fremde Kontrolle gerät. Angreifer können zum Beispiel die Funktionen des Satelliten dauerhaft deaktivieren, den Treibstoffverbrauch steuern, oder Sensoren beschädigen. Weiter wird der Transport der Satelliten in den Weltraum häufig von Dritten durchgeführt, was eine physische oder auch digitale Einflussnahme durch Dritte ermöglicht. All diese Einwirkungen können grundsätzlich die Cyberkomponente des Satelliten beeinflussen und dessen Funktionieren stören oder verhindern. Dieses Risiko ist erhöht, wenn Satelliten mehrere Dienste für mehrere Anbieter gleichzeitig ausführen. Das Teilen eines Satelliten mit möglicherweise nicht vertrauenswürdigen Entitäten erhöht z. B. das Risiko, dass böswillige Akteure ein Datenleak verursachen, in dem sie Informationen über sogenannte Seitenkanäle ableiten.

Die Schwachstellen von Software- und Hardwarekomponenten sind in allen Bereichen ein Thema, nicht nur im Weltraumsegment. Da jedoch im Weltraumsegment manipulierte oder defekte Software- und Hardwarekomponenten nur in den seltensten Fällen und unter sehr grossem Aufwand ersetzt werden können, muss hier solchen Schwachstellen besondere Beachtung geschenkt werden. Fortschritte im Bereich des In-Orbit Servicing (Wartung im Weltraum) könnten die Schwachstellenbehebung im Weltraumsegment in Zukunft verbessern. In-Orbit Servicing birgt aber gleichzeitig neue Risiken, da die entsprechenden Technologien auch für Angriffe missbraucht werden können.

Die vorgesehene Nutzung des Satelliten hat einen Einfluss auf die eingesetzte Hard- und Software, die Erdumlaufbahn, in welcher der Satellit stationiert wird, und die Bauweise des Satelliten. Erdnahe Satelliten sind in der Regel kleiner und werden mehrheitlich kommerziell genutzt. Ihre Lebensdauer ist kürzer und die Lancierungs- und Betriebskosten sind niedriger. Beim Bau von diesen Satelliten werden häufig kommerzielle Standardkomponenten (Commercial off-the-shelf, COTS) und Halbleiterchips aus der Automobil- und Mobiltelefonindustrie verwendet. Bei der Entwicklung dieser Komponenten und Chips werden die Anforderungen und die Bedrohungslandschaft für das Weltraumsegment nicht berücksichtigt. Um den mit der Verwendung von COTS-Komponenten ausgehenden Risiken zu begegnen, sind entsprechende Massnahmen bei der Auswahl und dem Einsatz von COTS-Komponenten zu berücksichtigen.[54]

Diese Verletzlichkeit durch die Verwendung von COTS-Komponenten wird von führenden Herstellern berücksichtigt. Kommerzielle LEO-Satelliten werden durch iterative Zyklen in höheren Quantitäten produziert, sind dadurch grundsätzlich jünger als staatliche Satelliten und weisen einen höheren Schutz gegen Cyberbedrohungen auf.[55] Der Einsatz der kommerziellen Satellitenkonstellation, die im Ukraine-Krieg eine zuverlässige, redundante Informations- und Kommunikationsstruktur bot, stellte die hohe Cybersicherheit von kommerziellen LEO-Satelliten unter Beweis. Trotz zahlreicher Cyberangriffe und Störungsversuche der Datenverbindung blieb die Satellitenkonstellation dank regelmässiger Software-Upgrades widerstandsfähig.[56]

Im Gegensatz zu den LEO-Satelliten werden für längerfristige Aufgaben in weiter entfernten Orbits teurere und grössere Satelliten gebaut.[57] Ihr Bau und ihre Lancierung sind aufwendig und bieten dadurch mehr Anreize, Cyberrisiken missionsspezifisch zu berücksichtigen. Allfällige Schwachstellen, die nicht vom Boden aus behoben werden können, sind aufgrund der längeren Lebensdauer länger exponiert, was ihre Entdeckung durch Angreifer wahrscheinlicher macht. Das Cyberrisiko von Schwachstellen in Cyberinfrastruktur ist daher besonders für komplexe und teure Satelliten relevant.

---

[52] Bundesamt für Bevölkerungsschutz BABS, Gefährdungsdossiers und Szenarien, <https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html#ui-collapse-743> (besucht am 20. Februar 2023).

[53] Sonnenstürme können Schäden bei der Weltrauminfrastruktur sowie bei terrestrischer kritischer Infrastruktur, wie die Stromversorgungsnetzwerke, zufügen. Neben bekannten Schäden an eben solchen terrestrischen kritischen Infrastrukturen könnten Sonnenstürme auch spezifisch terrestrische Cyberinfrastrukturen beschädigen, wie Unterseekabel. Diese Schäden könnten zu langfristigen Ausfällen des Internets führen. SANGEETHA ABDU JYOTHI, Solar Superstorms: Planning for an Internet Apocalypse, SIGCOMM, 2021, <https://www.ics.uci.edu/~sabdujyo/papers/sigcomm21-cme.pdf>; DAISY DOBBRIJEVIC. Coronal mass ejections: What are they and how do they form?, Space.com, 2022, <https://www.space.com/coronal-mass-ejections-cme> (besucht am 10. Februar 2023).

[54] PETER MATTHEWS, The Great Debate: Should COTS Components Be Used in Space?, Microwave Journal, 2022, <https://www.microwavejournal.com/articles/38974-the-great-debate-should-cots-components-be-used-in-space>; CHEN/HODSON, NESC Assessment – Recommendations on Use of Commercial-Off-The-Shelf (COTS) Parts for NASA Missions, NTRS – NASA Technical Reports Server, 2022, <https://ntrs.nasa.gov/search?q=20205011579>.

[55] Z. B. bei Satelliten der Hersteller SpaceX (Starlink), Spire (LEMUR) oder Planet (Flock).

[56] TARIQ MALIK, Elon Musk Says SpaceX Focusing on Cyber Defense After Starlink Signals Jammed Near Ukraine Conflict Areas, Space.com, 2022, <https://www.space.com/elon-musk-spacex-starlink-cyber-defense-ukraine-invasion>.

[57] Mit Ausnahme von geostationären Satelliten. Diese sind auf einer weiten Erdumlaufbahn stationiert (35'786 km), zählen aber auch zur Kategorie von Satelliten mit kommerzieller Mission. Sie werden mehrheitlich für Kommunikationsdienste genutzt. Ausführung zu Satelliten-Erdumlaufbahnen siehe Glossar.

Zusätzlich zu den bereits erwähnten Risiken und Risikofaktoren tragen verschiedene Trends zu einem erhöhten Bedarf an Cybersicherheit für Satelliten bei. Zu diesen Trends gehören softwaredefinierte Satelliten, Satellitenkonstellationen, verbesserte Sensorfähigkeiten bei kleinen und grossen Satelliten und maschinelles Lernen direkt auf der Satelliteninfrastruktur. Softwaredefinierte Satelliten erlauben die ferngesteuerte Konfiguration eines Satelliten. Diese kann jedoch nicht nur durch den eigentlichen Nutzer ausgeführt werden, sondern auch durch einen Angreifer. Satellitenkonstellationen, die aus einem Netz identischer oder gleichartiger Satelliten mit demselben Zweck und gemeinsamer Steuerung bestehen, können es einem Angreifenden erlauben, mit einer einzigen Aktion die Kontrolle über die gesamte Satellitenkonstellation zu erlangen. Verbesserte Sensorfähigkeiten, gerade bei kleinen (insb. LEO-)Satelliten, machen Satelliten bei der Datensammlung effizienter. Diese gesteigerten Fähigkeiten machen Satelliten zu immer attraktiveren Angriffszielen. Auch das maschinelle Lernen direkt auf den Satelliten kann aufgrund zusätzlicher Angriffsmöglichkeiten, z. B. über die zum Lernen genutzten Daten, zur Angriffsattraktivität beitragen. Weitere Risiken entstehen beim maschinellen Lernen auf Satelliten auch durch die Positionierung im Weltraumsegment, wie z. B. die beschränkte Überwachbarkeit und Beeinflussbarkeit des Lernprozesses im Gegensatz zum maschinellen Lernen am Boden.

3.2.3 Datenverbindung

Die Datenverbindungen zwischen dem Bodensegment und dem Weltraumsegment sowie Datenverbindungen innerhalb des Weltraumsegments (Satellit zu Satellit) können abgehört, umgeleitet, gestört, unterbrochen oder manipuliert werden. Die geringe Signalstärke an den Empfänger macht besonders die GNSS-Nutzung, und dabei insbesondere GPS-Signale, anfällig für Störung (Jamming) und Manipulation (Spoofing). Jamming kann absichtlich (böswillig), z. B. durch GNSS-Störsender, oder unbeabsichtigt durch die hohe Sendestärke von Radar- oder Kommunikationssystemen erfolgen. Aufgrund der Verwendung immer komplexerer Kommunikationsprotokolle setzen Angreifende «intelligentes» Jamming ein. Intelligentes Jamming erfordert weniger Leistung als konventionelles Jamming: Es maximiert seine Wirksamkeit durch gezielte Störsignale. GNSS-Spoofing ist die absichtliche Übertragung falscher GNSS-Signale, etwa, um den Nutzern eine wahre Position zu verschleiern. Spoofing ist schwieriger zu erkennen als Jamming, beinhaltet eine genaue Nachbildung der Signale und bedarf komplexer Gerätschaften.[58]
In Bezug auf Störungen und Unterbrüche der Datenverbindung ist insbesondere auch das Weltraumwetter als Risikofaktor zu berücksichtigen.[59]
Um die Datenverbindung gegen Abhörung und Manipulation zu schützen, wird im Gegensatz zur früheren Praxis die Datenverbindung vermehrt chiffriert. Dieser Schutz ist insbesondere für die über die Datenverbindung stattfindende Steuerung und Wartung der Weltraumgegenstände eines Weltraumsystems (z. B. Satelliten) relevant. Würde es Angreifern z. B. gelingen, bei einer Softwareaktualisierung eines Satelliten (Wartung), die über Datenverbindung erfolgt, eine manipulierte Software einzuspielen, stünden ihnen verschiedenste Arten der Einflussnahme offen.
In den letzten Jahren wird zunehmend Laser als Träger für die Datenübertragung zwischen Bodensegment und Satelliten oder zwischen Satelliten eingesetzt. Gegenüber der herkömmlichen Verwendung von sich kegelförmig ausbreitenden Funkwellen hat Laser sicherheitstechnische Vorteile: Ein Angreifer hat weniger Spielraum bezüglich seiner Position, wenn er die Datenverbindung abhören, umleiten, stören, oder unterbrechen möchte. Aus diesem Grund ist es auch sehr schwierig aufzuklären, woher und wohin Laserstrahlen gesendet werden.
Neben der Verwendung bewährter und zertifizierter kryptographischer Algorithmen zur Sicherung des Inhalts der Datenverbindungen, ist auch ein ganzheitliches Sicherheitskonzept vom Bodensegment bis zum Satelliten und zurück hilfreich. Dabei helfen Security by Design Prinzipien, d. h. Sicherheit wird schon von Beginn an in die Cyberinfrastruktur eingebaut. Zur Überprüfung der Umsetzung sollten zudem regelmässig sogenannte Penetrationstests durchgeführt werden, und allfällig entdeckte Schwachstellen sollten zeitnah behoben werden. Ebenfalls sollten zumindest sicherheitsrelevante und von den Herstellern zur Verfügung gestellte Patches, Updates und Upgrades zeitnah eingespielt werden.[60]

3.3 Fazit und mögliche Massnahmen

Die Weltrauminfrastruktur «Bodensegment – Datenverbindung – Weltraumsegment» weist in allen drei Segmenten viele verschiedene Cyberrisiken auf. Die Erhöhung der Sicherheit der einzelnen Elemente, z. B. durch die Umsetzung des Cybersicherheits-Frameworks empfohlen im NISTIR 8401 bei Bodensta-

[58] Jamming und Spoofing von GNSS-Signalen – ein unterschätztes Risiko?, Bodet Time, 2020, <https://www.bodet-time.com/de/zeitserver/artikel-und-ressourcen/1583-jamming-und-spoofing-von-gnss-signalen-ein-unterschaetztes-risiko.html>.

[59] Siehe Kapitel 3.2.2 «Weltraumsegment». Dieses Risiko gilt für alle Segmente der Weltrauminfrastruktur.

[60] Definition Patches, Updates, Upgrades siehe Glossar.

tionen[61], sowie die Stärkung des Gesamtsystems, z. B. durch die Berücksichtigung der Risiken und Empfehlungen der CCSDS für Weltraummissionen[62], trägt zu einer Verringerung der Anzahl und der Auswirkung von Cyberrisiken bei. Dabei gilt es, alle Glieder der Kette – von der sicheren Produktion, über den Betrieb und die Nutzung bis zur Entsorgung – zu kennen und möglichst sicher zu gestalten. In Anbetracht der Fallbeispiele des Ukraine-Kriegs für Cyberrisiken im Konfliktfall sind insbesondere auch kommerzielle Technologien in zivilen und militärischen Einsätzen für Dienstleistungen an kritischen Infrastrukturen zu sichern. Solche Dual-Use-Technologien, die in Weltrauminfrastrukturen eingesetzt werden, sollten entsprechende Sicherheitsvorkehrungen für militärische Angriffsziele erfahren.[63]

Die Schweiz hat mit einem vergleichsweise kleinen und wenig versorgungs- und sicherheitskritischen nationalen Bestand an Weltrauminfrastruktur nur begrenzte Möglichkeiten, deren Cybersicherheit zu stärken. Als Forschungs- und Entwicklungsstandort eröffnen sich jedoch mehrere Handlungsfelder. Konkrete mögliche Massnahmen für die Schweiz sind (1) die Erhöhung der Cybersicherheit aller Software- und Hardwarekomponenten durch die Anwendung von Security by Design Prinzipien in der Entwicklungsphase, (2) schweizweite Anreize oder Auflagen für private Hersteller und Betreiber der Weltrauminfrastruktur für Lieferketten- und Netzwerksicherheit.[64]
Diese möglichen Massnahmen sind dem strategischen Ziel «Sichere und verfügbare digitale Dienstleistungen und Infrastruktur» der NCS zuzuordnen. Sie präzisieren einen Schwerpunkt der Massnahme 6 «Resilienz, Standardisierung und Regulierung» – die Prüfung der Notwendigkeit von sektorspezifischen Regulierungen und wo nötig, die Ausarbeitung von entsprechenden Vorlagen – für den Forschungs- und Entwicklungsstandort Schweiz für Weltrauminfrastruktur.[65] Die möglichen Massnahmen unterstreichen dabei einen Grundsatz der NCS: der Schutz der Schweiz vor Cyberbedrohungen ist eine gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat.[66]

4 Der Handlungsspielraum und die Einflussnahme der Schweiz in internationalen Organisationen und Gremien

Die Abhängigkeit der Schweiz von Weltraumdienstleistungen nimmt zu (siehe Kapitel 2). Die Schweiz begegnet der damit einhergehenden zunehmenden Verletzlichkeit durch Cyberrisiken einerseits durch die Stärkung ihrer Resilienz und der Sicherheit ihrer Infrastrukturen sowie durch internationale Partnerschaften und der Teilnahme an internationalen Programmen und Organisationen.
Die Schweiz engagiert sich in internationalen Organisationen und Gremien in den Bereichen Weltraum und Cybersicherheit. Der Bundesrat hat dafür auf verschiedenen Verwaltungsebenen und für verschiedene Aspekte der Querschnittsthemen strategische Stossrichtungen festgehalten. Dazu gehören unter anderem die übergreifende NCS, die Strategie Cyber VBS, die Aussenpolitische Strategie 2020-2023, die Strategie Digitalaussenpolitik 2021-2024, die Strategie Rüstungskontrolle und Abrüstung 2022-2025, die Nationale Strategie zum Schutz kritischer Infrastrukturen und die Schweizer Weltraumpolitik 2023.
Grundsätzlich werden die Themen Weltraum und Cyber in internationalen Gremien bisher separat behandelt. Es existiert kein multilaterales Gremium, das sich in der Hauptsache und spezifisch mit der Schnittstelle der Bereiche Weltraum und Cybersicherheit beschäftigt. Stattdessen befassen sich viele internationale Organisationen oder Initiativen aus dem Weltraumbereich in Unterausschüssen mit Cybersicherheit. Dieser Bericht beschränkt sich in seiner Ausführung im Kapitel 4.1 auf diese Organisationen und Initiativen, die sich mit Weltraumthemen oder mit der Schnittstelle Weltraum-Cybersicherheit befassen.
In einigen internationalen und regionalen multilateralen Organisationen und Gremien wird Cybersicherheit hauptthematisch behandelt. Die Schweiz beteiligt sich aktiv an diesen Prozessen, zu deren Erfolg

[61] National Institute of Standards and Technology Interagency Report 8401. Das National Institute of Standards and Technology (NIST) ist ein staatliches Labor der Vereinigten Staaten, das für Bundesbehörden und andere Organisationen bewährte Verfahren in Bereichen wie Cybersicherheit entwickelt, testet und empfiehlt. NIST-interne oder behördenübergreifende Berichte (NISTIRs) beschreiben Forschungsarbeiten technischer Natur. Die Reihe umfasst Zwischen- oder Abschlussberichte über Arbeiten, die das NIST für externe Sponsoren (sowohl staatliche als auch nichtstaatliche) durchführt.

[62] Siehe auch z. B. die Empfehlungen des US White House Memorandum on Space Policy Directive 5 «Cybersecurity Principles for Space Systems». Security Threats Against Space Missions Informational Report, 2022; The White House, Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, 2020, <https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>.

[63] Definition Dual-Use siehe Glossar. BOSCHETTI/GORDON/FALCO, Space Cybersecurity Lessons Learned from the ViaSat Cyberattack, ASCEND, 2022, <https://arc.aiaa.org/doi/pdf/10.2514/6.2022-4380>.

[64] NAYEF AL-RHODAN, Cyber security and space security, 2020, <https://www.thespacereview.com/article/3950/1> (besucht am 12. Dezember 2022).

[65] Nationale Cyberstrategie NCS, 2023, S. 20-21.

[66] Nationale Cyberstrategie NCS, 2023, S. 12.

sie in den letzten Jahren massgeblich beigetragen hat.[67] Diese Gremien behandeln jedoch hauptsächlich umfassende Massnahmen der Cybergouvernanz und Cybersicherheit und gehen selten auf sektorspezifische Anliegen ein.

4.1 Vertretung der Schweiz in Organisationen und Gremien zu Weltraumthemen

Im Folgenden werden Organisationen und Gremien aufgeführt, welche sich mit Weltraumthemen oder mit der Schnittstelle Weltraum-Cybersicherheit befassen und in denen die Schweiz vertreten ist.[68]

Organisation	Auftrag Organisation und Gremium im Weltraum und Rolle der Schweiz
European Space Agency (ESA)	Die Europäische Weltraumorganisation (ESA) koordiniert die Zusammenarbeit in Europa auf dem Gebiet der Weltraumforschung und die kommerzielle Nutzung des Weltraumes. Die Schweiz ist Gründungsmitglied der ESA und leistet einen jährlichen Beitrag von ca. 195 Millionen Schweizer Franken an die Programme und Tätigkeiten der ESA. Die Schweiz leistet durch ihre Mitgliedschaft und durch ihre Beteiligung an den EU-Programmen (siehe unten) einen bedeutenden Beitrag zur europäischen Raumfahrt und trägt zur Weiterentwicklung zur europäischen Weltraumgouvernanz bei. Sie stellt dadurch den Zugang der Schweizer Wirtschaft und Wissenschaft zu internationalen Beschaffungsverfahren sicher. Im Rahmen der ESA beteiligt sich die Schweiz auch an der Entwicklung von EU-Flaggschiffprogrammen wie Copernicus oder Secure «IRIS²» (siehe Kapitel 5).
	Schnittstelle Weltraum-Cybersicherheit: Die ESA führt gebündelt Aktivitäten im Bereich Weltraum-Cybersicherheit durch, um einerseits ihre eigenen Systeme zu schützen und andererseits die entsprechenden Fähigkeiten der Mitgliedstaaten zu fördern.[69] Die Organisation verfügt über eine Strategie zu Cybersicherheit, welche voraussichtlich Ende 2023 publiziert werden wird.

[67] Die UNO behandelt Cybersicherheit in separaten Prozessen, zu deren Erfolge die Schweiz in den letzten Jahren massgebend beigetragen hat, namentlich durch die Leitung der «UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security» 2019 bis 2020 und einer Beteiligung in der «UN-Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace» 2019 bis 2021. In diesen Foren setzt sich die Schweiz für ein freies, offenes und sicheres Cyberspace ein. Konkret setzt sich die Schweiz für die Umsetzung des Rahmenwerkes für verantwortungsvolles Staatenverhalten im Cyberraum ein. Sie engagiert sich insbesondere für die Anwendung und Konkretisierung der bestehenden Regeln des Völkerrechts im Cyberspace, einschliesslich des humanitären Völkerrechts und der Menschenrechte. Auf europäischer Ebene ist die Schweiz in der OSZE aktiv und beteiligt sich an der Umsetzung vertrauensbildender Massnahmen im Cyberraum. Ausserdem ist die Schweiz aktiv im Bereich des Cyber-Kapazitätsaufbaus, z. B. als Mitglied des «Global Forum on Cyber Expertise (GFCE)».

[68] Die Liste ist nicht abschliessend.

[69] Vgl. European Space Agency, Cybersecurity, <https://technology.esa.int/program/cybersecurity> (besucht am 21. Juni 2022).

EU Agency for the Space Programme (EUSPA)	Die Agentur der EU für das Weltraumprogramm (EUSPA) ist in den Bereichen Erdbeobachtung, Satellitennavigation, Konnektivität, Weltraumforschung und Innovation aktiv und unterstützt Investitionen in kritische Infrastrukturen und Technologien. Weiter betreut die EUSPA Aufgaben im Bereich der Programmkomponenten der staatlichen Satellitenkommunikation der Europäischen Union (European Union Governmental Satellite Communications, GOVSATCOM; Copernicus), und ist Ansprechpartnerin für den Betriebsdienst «Space Surveillance and Tracking» der EU (EU SST). Die Schweiz ist in der EUSPA nicht vertreten. Die Schweiz ist jedoch an der EUSPA-Komponente des EU-Weltraumprogramms für Satellitennavigation (Galileo und EGNOS) direkt beteiligt. Die EU delegiert Forschungs- und Entwicklungsaktivitäten im Bereich ihres Raumfahrtprogramms an die ESA (siehe oben) und den Betrieb der Systeme an die EUSPA. Das GNSS-Abkommen zwischen der EU und der Schweiz sieht vor, dass die Schweiz an der EUSPA teilnehmen kann.[70] Die genauen Modalitäten der Schweizer Teilnahme an der EUSPA sind in einem Zusatzabkommen festzulegen. Ein Abkommensentwurf liegt vor. Die Unterzeichnung des Abkommensentwurfs wird jedoch von der EU unter Hinweis auf die offenen institutionellen Fragen blockiert. Eine frühzeitige Positionierung und Entwicklung von Schlüsselkomponenten, insbesondere über ESA-Programme, ist für die Einflussnahme der Schweiz zentral.[71] Der Bundesrat hat am 16. Februar 2022 entschieden und am 21. Juni 2023 bekräftigt, dass die Schweiz eine Teilnahme am EU-Erdbeobachtungsprogramm Copernicus anstrebt.[72] **Schnittstelle Weltraum-Cybersicherheit:** Die EUSPA führt zum Schutz der EU-Weltraumkomponenten Aktivitäten operationeller Sicherheit, Sicherheitstechnik und Cybersicherheit aus.
European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT)	Die Europäische Organisation für die Nutzung meteorologischer Satelliten (EUMETSAT) betreibt meteorologische Satelliten und stellt die Beobachtungsdaten den Mitgliedstaaten zur Verfügung. Die Schweiz ist Mitglied der EUMETSAT und wird durch MeteoSchweiz vertreten.
International Telecommunications Satellite Organization (ITSO), International Mobile Satellite Organization (IMSO) und European Telecommunications Satellite Organization (EUTELSAT IGO)	Die zwischenstaatlichen Satellitenorganisationen ITSO, IMSO und EUTELSAT IGO überwachen die Dienstleistungen der privaten Anbieterinnen von Satellitenkommunikationsdiensten Intelsat Ltd, Inmarsat plc und Eutelsat SA im Bereich Service public.[73] ▪ **ITSO:** Die Internationale Fernmeldesatellitenorganisation (ITSO) erbringt internationale öffentliche Fernmeldedienste von hoher Qualität und Zuverlässigkeit und fördert diese, um die Bedürfnisse der Informations- und Kommunikationsgesellschaft zu erfüllen. Die ITSO überwacht Intelsat Ltd. Sie zählt 149 Mitgliedstaaten. ▪ **IMSO:** Die Internationale Mobilfunksatellitenorganisation (IMSO) kontrolliert, dass die im weltweiten Seenot- und Sicherheitsfunksystem (GMDSS) von Inmarsat plc erbrachten mobilen Satellitenkommunikationsdienste den Regeln der Internationalen Seeschifffahrts-Organisation (IMO) entsprechen. Ausserdem koordiniert sie das von der IMO geschaffene System zur Identifizierung und Verfolgung von Schiffen über grosse Entfernungen (Long-Range Identification and Tracking). Sie zählt 104 Mitgliedstaaten. ▪ **EUTELSAT IGO:** Die Europäische Fernmeldesatellitenorganisation EUTELSAT IGO überwacht, ob die Eutelsat SA bei ihren Tätigkeiten die Grundsätze des Service public bzw. der Grundversorgung, der gesamteuropäischen Versorgung mit dem Satellitensystem, der Nichtdiskriminierung und des fairen Wettbewerbs einhält. Sie zählt 49 Mitgliedstaaten. Die Schweiz ist Mitgliedstaat von ITSO, IMSO und EUTELSAT IGO.

[70] Das GNSS-Abkommen ist ein Kooperationsabkommen zwischen der EU und der Schweiz, welches der Schweiz die Teilnahme an den europäischen Satellitennavigationsprogrammen Galileo und EGNOS ermöglicht.

[71] Die EUSPA ist z. B. auch an der Initiative zur Entwicklung eines EU Secure Connectivity Programms im Weltraum involviert, wie auch diverse andere EU-Programme/Gremien, die dadurch mitentwickelt werden (z. B. von Horizon Europe, CEF oder DEP Programmen). EUR-Lex, Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027, 2022, <http://data.europa.eu/eli/reg/2023/588/oj>.

[72] Medienmitteilung des Bundesrates vom 16. Februar 2022, Bundesrat strebt Teilnahme an Copernicus an, abrufbar unter: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-87213.html>.

[73] Definition Service public siehe Glossar.

Conférence Européenne des Administrations des Postes et des Télécommunications (CEPT)	Die Europäische Konferenz der Verwaltungen für Post und Telekommunikation (CEPT) setzt sich für die Schaffung dynamischer Märkte in den Bereichen Post und Telekommunikation in Europa ein.[74] Die Schweiz ist Gründungsmitglied der CEPT und beteiligt sich aktiv an der Ausgestaltung einer europäisch harmonisierten Funkfrequenzregulierung im Satellitensektor. Sie nimmt damit einen direkten Einfluss auf die in Europa und in der Schweiz nutzbaren Satellitendienste.
European Defence Agency	Die Europäische Verteidigungsagentur für die Bereiche Entwicklung der Verteidigungsfähigkeiten, Forschung, Beschaffung und Rüstung ist eine 2004 gegründete intergouvernementale Agentur der EU für Rüstungsplanung, -beschaffung und -forschung. Die Schweiz hat ein Framework for Cooperation mit der Europäischen Verteidigungsagentur und nimmt in diesem Rahmen Einsitz in der Ad Hoc Working Group on Space.[75]
UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS)	Der Ausschuss der Vereinten Nationen für die friedliche Nutzung des Weltraums (UNCOPUOS) fördert die internationale Zusammenarbeit bei der friedlichen Nutzung des Weltraums und klärt rechtliche Fragen, die sich aus der Nutzung des Weltraums ergeben. Auf Empfehlungen von UN COPUOS wurden z. B. das International Committee on GNSS (ICG) und die International Space Weather Initiative gegründet. Die Schweiz hat vier der fünf internationalen Weltraumverträge, die von UNCOPUOS entwickelt wurden, in den 1960er und 1970er Jahren ratifiziert. Diese Verträge regeln die Hauptprinzipien der Erforschung und der Nutzung des Weltraums sowie spezifischen Aspekte wie die staatliche Verantwortung und die Registrierung im UNO-Register für Weltraumgegenstände. Die Schweiz wurde 2008 Mitglied von UNCOPUOS, um bei der globalen Gouvernanz von Weltraumaktivitäten mitzuwirken. Sie fördert gemeinsame Regeln zur friedlichen, sicheren und nachhaltigen Nutzung des Weltraums sowie die Anwendung von Weltraumtechnologien zur nachhaltigen Entwicklung, u. a. im Gesundheitsbereich, und sitzt in den entsprechenden Arbeits- und Expertengruppen ein. So hat die Schweiz beispielsweise an der Ausarbeitung der Vereinten Nationen (UNO) Leitlinien zur langfristigen Nachhaltigkeit von Weltraumaktivitäten mitgewirkt.[76] **Schnittstelle Weltraum-Cybersicherheit:** Die friedliche und störungsfreie Führung von Weltraumaktivitäten (ohne Cyberinterferenzen) sowie die Mitigation von Weltraumwettereffekten sind Bestandteil des Aufgabenbereiches von UNCOPUOS.
UN General Assembly (UNGA) und United Nations Conference on Disarmament	Zusätzlich zum Engagement der Schweiz bei der UNO-Generalversammlung (UNGA) über die friedliche, sichere (i. S. von «safety») und nachhaltige Nutzung des Weltraums (4. Komitee), setzt sich die Schweiz für das Thema Weltraumsicherheit (i.S. von «security»)(1. Komitee) ein. Dazu engagiert sie sich unter anderem im Rahmen der von der UNO-Generalversammlung eingesetzten Arbeitsgruppe «Open-ended Working Group on Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviors» (OEWG Space Threats) für die Entwicklung von Prinzipien eines verantwortungsvollen Verhaltens im Weltraum.[77] Im Rahmen der Genfer Abrüstungskonferenz befürwortet die Schweiz die Aufnahme von Verhandlungen, um einen Rüstungswettlauf im Weltall zu verhindern (Prevention of an Arms Race in Outer Space, PAROS). Sie erachtet den von Russland und China im Jahr 2008 eingebrachten und 2014 aktualisierten Vertragsentwurf über die Stationierung von Waffen im Weltall und über die Verhinderung der Gewaltanwendung gegen Weltraumgegenstände (Draft Treaty on the Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force against Outer Space Objects, PPWT) als konstruktive Grundlage für die Aufnahme von Verhandlungen. Die seit 20 Jahren andauernde Blockade in diesem Gremium erschwert jedoch nach wie vor jeglichen Fortschritt in diesem Bereich. **Schnittstelle Weltraum-Cybersicherheit:** Die zunehmende Abhängigkeit von Weltraumdienstleistungen und die resultierende gesteigerte Verletzlichkeit durch Cyberrisiken, ist Bestandteil der Diskussionen im Rahmen der OEWG Space Threats, wo u. a. der Schutz terrestrischer (Cyber-)Infrastruktur thematisiert wird.

[74] Bundesamt für Kommunikation, CEPT – Europäische Konferenz der Verwaltungen für Post und Fernmeldewesen, <https://www.bakom.admin.ch/bakom/de/home/das-bakom/internationale-aktivitaeten/taetigkeiten-des-bakom-in-internationalen-organisationen/cept.html> (besucht am 10. Januar 2023).

[75] European Defence Agency, Ad Hoc Working Group Space, <https://eda.europa.eu/what-we-do/all-activities/activities-search/ad-hoc-working-group-space> (besucht am 2. Februar 2023).

[76] Die von UNCOPUOS entwickelten "UN Guidelines on the Long-term Sustainability of Outer Space Activities" (A/74/20, Annex II) wurden von der UNO-Generalversammlung gutgeheissen (A/RES/74/82).

[77] A/RES/76/231.

World Meteorological Organization (WMO)	Die Weltorganisation für Meteorologie (WMO) zielt mit ihrem «WMO Space Programme» u. a. auf die Errichtung eines globalen Wetter-Beobachtungssystems ab und hat eine Weltraumwetter-Expertengruppe geschaffen. Ausserdem unterstützt das Programm die Umsetzung internationaler Übereinkommen im Umweltbereich.[78] Die Schweiz ist Mitglied der WMO.
International Telecommunication Union (ITU)	Die Internationale Fernmeldeunion (ITU) ist eine Unterorganisation der UNO. Der Radiosektor der ITU (ITU-R) stellt durch regulatorische und technische Massnahmen sicher, dass der internationale Funkverkehr (inklusive Satellitenkommunikation) grenzüberschreitend störungsfrei betrieben werden kann. Die ITU ist für die internationale Koordination aller Satelliten zuständig. Diese Koordination beinhaltet die Funknutzung und die Orbitalpositionen aller Satelliten. Die Schweiz ist Mitglied der ITU.
	Schnittstelle Weltraum-Cybersicherheit: Das ITU Radioreglement für den Funkdienst hat mehrere Bestimmungen zum Schutz vor funktechnischen Störungen des Funkdienstes und der Kommunikation erlassen, die von den Mitgliedsstaaten einzuhalten sind. Studiengruppen («Study Groups») in den Abteilungen der Radiokommunikation, Standardisierung, und Entwicklung veröffentlichen technische Studien oder Standards zur Cybersicherheit der Weltrauminfrastruktur.[79]

4.2 Fazit und mögliche Massnahmen

Seit den 1960er-Jahren gestaltet die Schweiz den Weltraum und die Raumfahrt in internationalen Gremien und Organisationen mit. Um ihre Interessen zu wahren, ist die Schweiz auf die internationale Zusammenarbeit angewiesen und ist als zuverlässige Akteurin international anerkannt. Die Schweiz engagiert sich aktiv in verschiedenen UNO-Gremien, sei es in den Bereichen friedliche, sichere und nachhaltige Nutzungen des Weltraums, Weltraumgouvernanz (UNCOPUOS und UNGA), der Koordination der Funknutzung und der Orbitalpositionen aller Satelliten (ITU) oder Meteorologie (WMO) und Weltraumwetter (WMO und UNCOPUOS). Die Schweiz ist in zahlreichen Organisationen und Gremien vertreten, welche sich mit Weltraumthemen, mit der Schnittstelle Weltraum-Cybersicherheit oder mit der Stärkung der Cybergouvernanz und der Cybersicherheit befassen. [80]
Als Gründungsmitglied der vorgestellten zwischenstaatlichen Organisationen wie der ESA oder EUMETSAT und dank der Teilnahme an einzelnen Komponenten des EU-Weltraumprogramms kann die Schweiz die internationale Raumfahrtinfrastruktursysteme mitgestalten und hat grundsätzlich Zugang zu den für sie wichtigen Infrastrukturen und den daraus abgeleiteten Daten sowie Dienstleistungen. Dank der internationalen Zusammenarbeit bei der Entwicklung und dem Betrieb von Weltrauminfrastrukturen können einzelne Staaten wie die Schweiz die volle Leistung der Raumfahrtinfrastruktursysteme nutzen, obwohl sie nur einen Teil davon finanzieren.
Mögliche Massnahmen für eine Ausweitung des Handlungsspielraums der Schweiz in internationalen Organisationen und Gremien sind verschiedenen strategischen Dokumenten des Bundesrates zu entnehmen. Die Schweiz soll ihren Status in internationalen Organisationen als zuverlässige Akteurin wahren und sich weiterhin in internationalen Foren für die Beachtung des Völkerrechts und dessen Weiterentwicklung innerhalb der Staatengemeinschaft einsetzen. Die Schweiz engagiert sich für eine friedliche und sichere Nutzung des Weltraums sowie die langfristige Nachhaltigkeit von Weltraumaktivitäten für die Verringerung der Bedrohungen im und aus dem Weltraum, und für transparentes und verantwortungsvolles Verhalten bei allen weltraumbezogenen Tätigkeiten.[81] Dazu setzt sich die Schweiz für weltweit geltende Regeln, Normen und Leitlinien ein. Auch soll die Schweiz durch Teilnahme in diesen internationalen Gremien und Foren die Entwicklungen in Bezug auf die militärische Nutzung des Weltraums vermehrt beobachten und beurteilen. In Bezug auf die Nutzung des Funkspektrums und der Orbitalpositionen wahrt die Schweiz ihre Interessen durch aktive Mitarbeit bei der Ausgestaltung der globalen Regulierung.[82]
Zusätzlich soll die Schweiz die internationale Zusammenarbeit im Raumfahrtbereich, insbesondere mit der ESA, EUMETSAT sowie der EU intensivieren. Der Zugang zu internationalen Beschaffungsverfah-

[78] World Meteorological Organization, WMO Space Programme (WSP), <https://community.wmo.int/en/activity-areas/wmo-space-programme-wsp> (besucht am 20. Juli 2023).

[79] Z. B. ITU, Recommendation SA.2142, 2021, <https://www.itu.int/rec/R-REC-SA.2142/en>; ITU, Harmful Interference and Infringements of the Radio Regulations, 2013, < https://www.itu.int/en/ITU-R/terrestrial/workshops/RRS-13-Africa/Documents/Harmful%20Interference.pdf>; ITU BR-SSD e-Learning Center, Harmful Interference to Space Services, <https://www.itu.int/en/ITU-R/space/elearning/presentations/UIT_SSD_028.pdf>.

[80] Strategie Digitalaussenpolitik 2021-2024, S.17.

[81] Weltraumpolitik 2023, 2023, S. 17.

[82] Weltraumpolitik 2023, 2023, S. 20.

ren für Wirtschaft und Wissenschaft soll sichergestellt werden.[83] Mit einer noch stärkeren Teilnahme, insbesondere an internationalen Technologieentwicklungs- und Forschungsprogrammen, kann sich die Schweiz für den gemeinsamen Erfolg bei der Entwicklung und dem Betrieb von Weltrauminfrastrukturen einsetzen und so langfristig auch den Zugang zu diesen Infrastrukturen sicherstellen, ihre Interessen wahren und ihre Resilienz zu erhöhen.[84] Mit der Weltraumpolitik 2023 hat der Bundesrat zudem festgelegt, dass er grundsätzlich eine umfassende Teilnahme an der für die Schweiz relevanten Infrastrukturprogrammen anstrebt.
Mit der Entwicklung von Bausteinen und Schlüsseltechnologien der Weltrauminfrastruktur trägt die Schweiz dazu bei, dass die europäischen Raumfahrtinfrastrukturen global wettbewerbsfähig und autonom sind.[85] Dies kann zur Relevanz der Schweiz beitragen sowie nationale und internationale Ausstrahlungskraft besitzen.[86] Diese Massnahme unterstützt das grundlegende Ziel, die Präsenz und Sichtbarkeit der Schweiz in internationalen Foren und bei internationalen Veranstaltungen zu erhöhen. Dafür soll das Bundesaussennetz verstärkt und zur Anbahnung wirtschaftlicher und wissenschaftlicher Tätigkeiten genutzt werden.[87] Sowohl im bilateralen als auch im internationalen Rahmen sollen Netzwerke und Allianzen ermöglicht und gestärkt werden.
Diese möglichen Massnahmen sind verschiedenen strategischen Stossrichtungen, Zielen, Handlungsfeldern und Massnahmen strategischer Dokumente des Bundesrates zuzuordnen.[88] Hervorzuheben sind einerseits ein Ziel des Aktionsfeldes «Cyberraum und Weltraum» der Strategie Rüstungskontrolle und Abrüstung 2022-2025 und andererseits eine Umsetzungsmassnahme des Sicherheitspolitischen Berichtes 2021. Diese verlauten: «Die Schweiz setzt sich für die Stärkung und Weiterentwicklung der Gouvernanzinstrumente betreffend Weltraum ein»[89] und zur Stärkung der Resilienz und Versorgungssicherheit bei internationalen Konflikten dient die «Verstärkung des Zugangs zu weltraumbasierten Dienstleistungen zur Kommunikation, Navigation und Erdbeobachtung sowie des internationalen Engagements zur Stärkung der langfristigen und friedlichen Nutzung des Weltraums».[90] Die möglichen Massnahmen decken sich zudem grundsätzlich mit den strategischen Stossrichtungen «Zugang und Resilienz», «Wettbewerbsfähigkeit und Relevanz» und «Partnerschaft und Zuverlässigkeit» der Weltraumpolitik 2023.

5 Die Möglichkeit der Teilnahme an Europäischen Satellitenkommunikationssystemen

In der Schweiz wird Satellitenkommunikation nur punktuell staatlich eingesetzt.[91] Die Bundesverwaltung betreibt keine eigenen Satelliten. Der Satellitenkommunikation wird jedoch eine wachsende Bedeutung beigemessen, insbesondere im Sicherheitsbereich.[92]
Bei Satellitenkommunikationssystemen wird die Daten-, Bild- oder Tonübertragung zwischen Sendern und Empfängern mit Hilfe von Telekommunikationssatelliten sichergestellt. Das eigentliche Kommunikationssystem besteht dabei nebst den Satelliten aus einem Bodensegment zur Steuerung, Kontrolle, Vernetzung und Absicherung des Gesamtsystems sowie dem Nutzersegment, welches die eigentliche Kommunikation der (End-)Nutzer über die Satellitenverbindungen ermöglicht. Das Boden- und Benutzersegment sowie indirekt die Satelliten sind dabei meist Teil grösserer, auch terrestrisch vernetzter Kommunikationssysteme.
Im Hinblick auf die Fragestellung muss zwischen kommerziellen und staatlichen Satellitenkommunikationssystemen unterschieden werden. Erstere werden von kommerziellen Anbietern aufgebaut, betrieben und vermarktet, letztere stehen unter der Kontrolle und Hoheit staatlicher Akteure. Beide ermöglichen grundsätzlich unterschiedlichen Kundensegmenten die Nutzung der entsprechenden Kommunikationsdienste, eine staatlich-militärische Nutzung kommerzieller Satellitenkommunikationssysteme ist dabei ebenso denkbar wie eine private Nutzung eines staatlich aufgebauten und geführten Satellitenkommunikationssystems. Die Mehrheit der heutigen Satellitenkommunikationssysteme ist kommerzieller Natur, auf deren Kapazitäten auch staatliche Akteure zurückgreifen. In jüngerer Zeit hat namentlich die Nutzung von privaten Systemen durch die Verteidigungskräfte der Ukraine grosse Aufmerksamkeit erhalten.

[83] Weltraumpolitik 2023, 2023, S. 16.

[84] Weltraumpolitik 2023, 2023, S. 17.

[85] Z. B. mit den Nutzlastverkleidungen für die Trägerraketen Ariane und Vega oder den Atomuhren für das Satellitennavigationssystem Galileo.

[86] Weltraumpolitik 2023, 2023, S. 19.

[87] Ibid.

[88] Siehe Kapitel 1.1 «Strategische Ausgangslage Schweiz». U. a. Aussenpolitische Strategie 2020-2023, 2020, S. 15-20; der Sicherheitspolitische Bericht 2021, 2021, S. 10, 45; Strategie Digitalaussenpolitik 2021-2024, 2020, S. 9, 13; Strategie Rüstungskontrolle und Abrüstung 2022-2025, 2022, S. 30; Weltraumpolitik 2023, 2023.

[89] Strategie Rüstungskontrolle und Abrüstung 2022-2025, 2022, S. 30.

[90] Die Sicherheitspolitik der Schweiz Bericht des Bundesrates (2021) BBl 2021 2895, S. 45.

[91] Die Sicherheitspolitik der Schweiz Bericht des Bundesrates (2016) BBl 2016 7763.

[92] Die Sicherheitspolitik der Schweiz Bericht des Bundesrates (2021) BBl 2021 2895.

Vor dem Hintergrund einer zunehmend strategischen Sicht auf Satellitenkommunikationssysteme gibt es insbesondere in Europa vermehrt Bestrebungen, staatlich geführte Systeme oder Netzwerke von Satellitenkommunikationssystemen aufzubauen und staatlichen Nutzern zur Verfügung zu stellen.
Die Teilnahme an den europäischen Satellitenkommunikationssystemen, namentlich an den unterschiedlichen Entwicklungsprogrammen der ESA, bietet der Schweiz die Möglichkeit, sich frühzeitig mit Schlüsselkompetenzen zu positionieren, um sich sodann mit einzigartigen Beiträgen als verlässliche Partnerin und Nutzerin der operationellen Systeme einzubringen. Die Schweiz hat sich in der Vergangenheit für GOVSATCOM im Rahmen der EDA interessiert. In den letzten Jahren hat sich aus dieser Initiative jedoch keine Handlungsrichtung konkretisiert. Der Bundesrat strebt eine Teilnahme der Schweiz an Copernicus, dem Programm der EU zur Erdbeobachtung, in der aktuellen Programmperiode 2021–2027 an.[93] Eine Ausweitung der Schweizer Teilnahme am EU-Weltraumprogramm setzt die Aufnahme entsprechender Verhandlungen und spezifische Abkommen für eine Teilnahme an den zusätzlichen Programmkomponenten für Satellitenkommunikation voraus.[94] Die EU betrachtet die Zusammenarbeit mit der Schweiz im Rahmen der EU-Programme (inkl. Copernicus) im Lichte der Gesamtbeziehungen Schweiz-EU.
Auf bilateraler Ebene stehen sicherheitspolitisch schwergewichtig Kooperationsvereinbarungen mit westlichen Staaten und deren Industriepartnern im Vordergrund. Alle Kooperationen sind im Einzelfall auf ihre Übereinstimmung mit dem geltenden Rechtsrahmen, der Unabhängigkeit und der Neutralität der Schweiz zu überprüfen.

5.1 Programme mit Schweizer Beteiligung

Die Schweiz beteiligt sich heute an folgenden europäischen oder nationalen Programmen zur Entwicklung von Satellitenkommunikationssystemen und -diensten:

- ESA Programm für Forschung und Entwicklung von Telekommunikationssystemen (Advanced Research in Telecommunications Systems, ARTES), inklusive deren Anwendung, sowie spezifischen Initiativen für sichere Datenübermittlung in der Raumfahrt oder für Quantum Key Distribution (QKD),[95]
- ESA-Programm im Zusammenhang mit der «Infrastructure for Resilience, Interconnectivity and Security by Satellite» der EU («IRIS²», vormals «Secure Connectivity Initiative»),[96]
- ESA Europäisches Zentrum für Weltraumsicherheit und Ausbildung mit seinem Kompetenzzentrum für Cybersicherheit (Security Cyber Centre of Excellence), der zentralen Anlaufstelle für Cyber-Tests, Schulungen und Experimente für nicht klassifizierte und klassifizierte Entwicklungen in einer kontrollierten sicheren Umgebung,[97]
- Nationale Programme und Public-Private Partnerships (PPP) im Rahmen der ESA, namentlich die durch die Schweiz angeführte Entwicklung der Plattform HummingSat für kleine, auf 3D-Drucktechnologien basierende geostationäre Telekommunikationssatelliten.

5.2 Fazit und mögliche Massnahmen

Mögliche Massnahmen für die Teilnahme an europäischen Satellitenkommunikationen folgen den strategischen Zielen der Weltraumpolitik 2023, wissenschaftliche Exzellenz zu fördern, Wettbewerbsfähigkeit zu stärken und die Zusammenarbeit zu intensivieren.[98] Um den vollen Nutzen aus ihren Schlüsselkompetenzen in europäischen Entwicklungsprogrammen für Satellitenkommunikation zu ziehen, muss sich die Schweiz frühzeitig positionieren. Dazu gehört einerseits die Teilnahme an den Entwicklungsprogrammen der ESA im Bereich der (sicheren) Satellitenkommunikation für die Festigung und Weiterentwicklung der Schlüsselkompetenzen. Andererseits betrifft dies auch die Teilnahme an den relevanten

[93] Medienmitteilung des Bundesrates vom 16. Februar 2022, Bundesrat strebt Teilnahme an Copernicus an, abrufbar unter: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-87213.html>.

[94] Die Schweiz nimmt heute über das EGNSS Kooperationsabkommen vollumfänglich und zeitlich unbefristet am Programmteil «Galileo und EGNOS» des Europäischen Weltraumprogramms teil. Siehe dazu auch Kapitel 2.4.1. «Vertretung der Schweiz in Agenturen zu Weltraumthemen».

[95] ESA TIA, <https://artes.esa.int/>; ESA TIA, Space Systems for Safety and Security (4S), <https://artes.esa.int/space-systems-safety-and-security-4s>; ESA TIA, Quantum encryption to boost European autonomy, <https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Quantum_encryption_to_boost_European_autonomy>.

[96] Der Bundesrat, Die Schweiz beteiligt sich an neuen ESA-Programmen und setzt sich für die verstärkten Ambitionen der europäischen Raumfahrt ein, 2022, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-91890.html>; ESA, Ministers back ESA's bold ambitions for space with record 17% rise, 2022, <https://www.esa.int/About_Us/Corporate_news/Ministers_back_ESA_s_bold_ambitions_for_space_with_record_17_rise>; Council of the EU, Council and European Parliament agree on boosting secure communications with a new satellite system, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/11/17/council-and-european-parliament-agree-on-boosting-secure-communications-with-a-new-satellite-system/>; European Commission, IRIS²: the new EU Secure Satellite Constellation, <https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en>.

[97] Unter anderem können im Security Cyber Centre of Excellence in einer synthetischen Umgebung kritische betriebliche Anwendungen und Infrastrukturen nachgebildet werden, um sie anhand massgeschneiderter Cyber-Bedrohungsszenarien zu testen und validieren. Die Fähigkeiten des Kompetenzzentrums werden laufend erweitert und können von der ESA und ihren Partnern (Mitgliedstaaten) genutzt werden.

[98] Weltraumpolitik 2023, 2023, S. 18-19.

Komponenten des EU-Weltraumprogramms für den Zugang zu den Diensten und wiederkehrende Beschaffungen, die für die Schweizer Raumfahrtindustrie kommerziell wichtig sind. Die Schweiz soll sich als zuverlässige Partnerin und Nutzerin der operationellen Systeme einbringen.

6 Rechtliche Aspekte der Datenübermittlung im Weltraum

6.1 Die internationale Rechtslage bei der Datenübermittlung im Weltraum

Die Datenübermittlung im Weltraum ist in keinem spezifischen völkerrechtlichen Vertrag geregelt. Es gelten die allgemeinen Prinzipien des Völkerrechts, des internationalen Weltraumrechts sowie weitere besondere Regelwerke, etwa hinsichtlich des internationalen Fernmeldewesens.

Die Schweiz hat vier der fünf Weltraumverträge der UNO ratifiziert,[99] darunter der Weltraumvertrag von 1967, der von 113 Staaten ratifiziert wurde.[100] Zu den Grundprinzipien dieses Weltraumvertrags gehören die freie Erforschung und Nutzung des Weltraums durch alle Staaten (Art. I) sowie die Prinzipien von «gebührender Rücksichtnahme» und ohne Beeinträchtigung mit den Aktivitäten von anderen Vertragsparteien (Art. IX). Der Weltraumvertrag von 1967 hält fest, dass die Vertragsparteien die Erforschung des Weltraums einschliesslich des Mondes und anderer Himmelskörper in Übereinstimmung mit dem Völkerrecht einschliesslich der Charta der Vereinten Nationen im Interesse der Erhaltung des Weltfriedens und der internationalen Sicherheit ausüben (Art. III). Die Vertragsstaaten sind völkerrechtlich verantwortlich für nationalen Tätigkeiten im Weltraum, unabhängig davon, ob staatliche Stellen oder nichtstaatliche Rechtsträger dabei tätig werden (Art. VI). Inwieweit sich diese Grundprinzipien auch auf die Datenübermittlung im Weltraum erstrecken, ist völkerrechtlich nicht eindeutig geklärt, und es besteht zu dieser Frage weder eine Gerichts- noch eine ständige Staatenpraxis.
Neben den Grundprinzipien gelten internationale Regelwerke für die Schweiz. Die von der Schweiz ratifizierte ITU-Verfassung und die ITU-Konvention legen die Grundsätze der ITU fest, darunter ihre Rolle in den Bereichen der Standardisierung (ITU-T), der Entwicklung des Fernmeldewesens (Telecommunication Development Sektor, ITU-D) und des Funkverkehrs (ITU-R). Die ITU-R ist für die Frequenzzuweisung für weltweite Funkdienste zuständig, die in der Vollzugsordnung für den Funkdienst kodifiziert sind.[101] In Bezug auf weltraumgestützte Dienste wendet die ITU-R die internationalen Koordinierungs- und Registrierungsverfahren für Weltraumsysteme und Bodenstationen an, die nach Aufnahme der entsprechenden Funkfrequenzen in die Internationale Frequenzreferenzdatei (MIFR) international anerkannt werden. Sie verwaltet die entsprechenden Verfahren der ITU-Zuweisungs- oder Allokationspläne.[102]
Das von der Schweiz ratifizierte und implementierte Radioreglement (völkerrechtlicher Vertrag zwischen UNO-Mitgliedstaaten)[103] der ITU bildet die Grundlage für die effektive Koordination und Notifikation von Satelliten. Dies beinhaltet die Funknutzung und die Orbitalpositionen der Satelliten. Die Verfahren des Radioreglements gewährleisten die internationale Anerkennung und den regulatorischen Schutz von Satelliten.
Im Weiteren bestehen verschiedene Verträge der Schweiz mit internationalen Organisationen: Das Übereinkommen zur Gründung einer Europäischen Weltraumorganisation (ESA), deren Programme Forschungs- und Entwicklungstätigkeiten gewidmet sind sowie Verträge über den Betrieb von Weltraumsystemen wie beispielsweise die Übereinkommen zur Gründung der Internationalen Organisation für mobile Satellitenkommunikation (IMSO) und der Internationalen Fernmeldesatellitenorganisation (ITSO), der Europäischen Fernmeldesatellitenorganisation (EUTELSAT IGO) und der Europäischen Organisation für die Nutzung von meteorologischen Satelliten (EUMETSAT).

[99] Die Schweiz hat vier der fünf Weltraumverträge ratifiziert: Der Vertrag vom 27. Januar 1967 über die Grundsätze zur Regelung der Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschliesslich des Mondes und anderer Himmelskörper (SR 0.790), das Übereinkommen über die Rettung und die Rückführung von Raumfahrern sowie die Rückgabe von in den Weltraum gestarteten Gegenständen (SR 0.790.1), das Übereinkommen über die völkerrechtliche Haftung für Schäden durch Weltraumgegenstände (SR 0.790.2) und das Übereinkommen über die Registrierung von in den Weltraum gestarteten Gegenständen (SR 0.790.3).

[100] Stand Juni 2023 haben 113 Staaten den Vertrag über die Grundsätze zur Regelung der Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschliesslich des Mondes und anderer Himmelskörper (SR 0.790) ratifiziert. United Nations Office for Disarmament Affairs, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, <https://treaties.unoda.org/t/outer_space> (besucht am 24. Juli 2023).

[101] Art. 1.8 RR(2020) «space radiocommunication: Any radiocommunication involving the use of one or more space stations or the use of one or more reflecting satellites or other objects in space».

[102] Secteur des radiocommunications (UIT-R) (itu.int) www.itu-int>Radiocommunications.

[103] Radioreglement vom 17. November 1995 (SR 0.784.403.1).

In Bezug auf die Datenübermittlung im Weltraum bestehen darüber hinaus keine konkreten internationalen Verpflichtungen der Schweiz. Die Schweiz wird die juristischen Debatten in internationalen Foren über den rechtlichen Status der im Weltraum übertragenen und gespeicherten Daten im Auge behalten.[104] Sie ist in verschiedenen internationalen Gremien und Foren zu den Themen Cybergouvernanz und Cybersicherheit vertreten (siehe Kapitel 4) und beteiligt sich aktiv an diesen Prozessen. Obwohl diese Gremien hauptsächlich umfassende Massnahmen der Cybergouvernanz und Cybersicherheit behandeln, dürften die Ergebnisse dieser Diskussionen auch für die Datenübermittlung im Bereich Weltraum von Relevanz sein. Dabei ist auch der Ansatz zu beobachten, dass die Gesetzgebung über die Cybersicherheit im Weltraum sich nicht wesentlich von jener der Cybersicherheit auf der Erde unterscheidet. So können beispielsweise landesrechtliche zivil- oder strafrechtliche Bestimmungen auch auf Aktivitäten Anwendung finden, die sich im Weltraum abspielen.

6.2 Die Schweizer Rechtslage bei der Datenübermittlung im Weltraum

Der rechtliche Rahmen in der Schweiz für die Datenübermittlung im Weltraum ist über das Fernmeldegesetz (FMG) gesetzt.[105] Das Fernmeldegesetz enthält im Wesentlichen zwei Artikel, welche auch im Zusammenhang mit der Datenübermittlung über Satelliten von Bedeutung sind:

- Art. 43 Vertraulichkeit der Daten: Wer mit fernmeldedienstlichen Aufgaben betraut ist oder betraut war, darf Dritten keine Angaben über den Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern machen und niemandem Gelegenheit geben, solche Angaben weiterzugeben.
- Art. 48a Sicherheit: Das revidierte FMG verpflichtet in der Schweiz gemeldete Anbieterinnen von Fernmeldediensten (FDA) neu, sog. Cyber-Attacken zu bekämpfen. Hierfür bzw. zum Schutz der Anlagen sind FDA berechtigt, Verbindungen umzuleiten, zu verhindern oder Informationen zu unterdrücken. Der Bundesrat ist zudem ermächtigt, zum Schutz der Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten weitere Regelungen zu erlassen, insbesondere etwa hinsichtlich Verfügbarkeit und Betrieb von Anlagen oder der Sicherstellung von redundanten Infrastrukturen und der Meldung von Störungen. Dabei gilt es zu beachten, dass Satellitenbetreiber, welche in der Schweiz Fernmeldedienste erbringen, als FDA gemeldet sein müssen. Sie sind somit für die Integrität der durch sie übermittelten Daten verantwortlich.

Gemäss Artikel 25 FMG ist das Bundesamt für Kommunikation (BAKOM) für die Verwaltung der Frequenzressourcen zuständig. Das BAKOM erstellt unter Beachtung der internationalen Vereinbarungen und der relevanten Publikationen des Electronic Communications Committee (ECC) der CEPT den Nationalen Frequenzzuweisungsplan (NaFZ).[106] Die darin enthaltenen technischen und regulatorischen Rahmenbedingungen sind für sämtliche Nutzer des Funkspektrums (inkl. Satelliten) verbindlich. Der NaFZ wird jährlich durch den Bundesrat genehmigt. Individuelle Frequenznutzungsrechte werden den Nutzern in Form von Funkkonzessionen eingeräumt. In die Zuständigkeiten des BAKOM fallen auch die internationale Koordination und Notifikation von Satelliten für schweizerische Organisationen, Firmen beziehungsweise Behörden und Bodenstationen auf Schweizer Territorium. Als Grundlage für die Koordination und Notifikation von Satelliten dient das von der Schweiz ratifizierte und implementierte Radioreglement.[107]

Die von Satelliten abgestrahlten Funksignale sind auf der Erde wegen der grossen Distanz äusserst schwach. Um sie noch mit genügender Qualität zu empfangen, braucht es Richtfunkantennen, wie zum Beispiel die Parabolantennen, die zum Empfang von Satelliten-TV nötig sind. Sollen für die Internetnutzung Signale zurück in den Weltraum gesendet werden, braucht es ebenfalls Richtfunkantennen. Deren Strahlung wird durch das Umweltschutzgesetz (Artikel 11 Abs. 1 USG; SR 814.01) und die darauf basierende Verordnung über den Schutz vor nichtionisierender Strahlung (Anhang 1, Ziff. 61 ff. NISV; SR 814.710) begrenzt.[108]

Rechtliche Aspekte der Datenübermittlung, spezifisch bei Cyberrisiken im Weltraum, können auch andere Bereiche des öffentlichen Rechts tangieren, wie beispielsweise das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)[109] oder das neue Bundesgesetz vom 18. Dezember 2020 über die

[104] STEFAN SOESANTO, Terra Calling: Defending and Securing the Space Economy, ETH Zürich, 2021, <https://doi.org/10.3929/ethz-b-000460220>.

[105] Fernmeldegesetz vom 30. April 1997 (SR 784.10).

[106] Frequency Allocation Plan, <https://www.ofcomnet.ch/#/fatTable>.

[107] Radioreglement vom 17. November 1995, in Kraft getreten am 1. Juni 1998 (SR 0.784.403.1). Das Radioreglement wird anlässlich der Weltfunkkonferenzen regelmässig nachgeführt und jeweils anschliessend vom Bundesrat ratifiziert. <https://www.fedlex.admin.ch/eli/cc/2005/778/de>.

[108] Die Sendeantennen sollten derart installiert werden, dass sich niemand in deren Antennenstrahl begeben kann. Ausserhalb sind die Belastungen gering. Für die Bewilligung und Kontrolle sind die Kantone oder Gemeinden zuständig.

[109] SR 235.1.

Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)[110]. Je nach Fallkonstellation ist bei Cyberrisiken auch im Falle eines Handlungs- respektive Begehungsort im Weltraum nicht auszuschliessen, dass Bestimmungen des in der Schweiz massgebenden Zivil- und Strafrechts anwendbar sind, beispielsweise wenn sich die betreffenden Handlungen auf das schweizerische Territorium oder auf sich darauf befindende Personen oder Gegenstände auswirken.

6.3 Fazit und mögliche Massnahmen

Die Frage der Rechtslage bei der Datenübermittlung wird in Angesicht der Diversifizierung der Akteure im Weltraum durch den Ausbau kommerzieller weltraumbasierter Dienstleistungen komplexer, vergleichbar mit den Entwicklungen im Bereich Recht im Internet oder hinsichtlich der künstlichen Intelligenz.[111] Aufgrund der globalen Dimension der Thematik wird die Schweiz entsprechend die juristischen Debatten in internationalen Foren über den rechtlichen Status der im Weltraum übertragenen und gespeicherten Daten im Auge behalten.[112] In der Schweiz wird der rechtliche Rahmen für die Datenübermittlung im Weltraum primär über das Fernmeldegesetz (FMG) und weitere bundesrechtliche Erlasse gesetzt.

Angesichts der Entwicklungen im Raumfahrtsektor auf nationaler und internationaler Ebene hat der Bundesrat am 16. Februar 2022 beschlossen, neben der Aktualisierung der Weltraumpolitik eine Vernehmlassungsvorlage für ein Raumfahrtgesetz zu erarbeiten. Die Schweiz schafft damit für die von ihr ratifizierten Weltraumverträge der UNO einen nationalen Rechtsrahmen, der die Bewilligung und Aufsicht von Weltraumaktivitäten, Haftungsfragen und ein Register für Weltraumgegenstände umfasst.[113] Mit einem nationalen Raumfahrtgesetz kann die Schweiz nicht nur ihre internationalen Verpflichtungen in innerstaatliches Recht überführen, sondern auch die Rechtssicherheit in diesem Bereich für alle beteiligten Akteure verbessern.[114] Datenübermittlungsrelevante Fragen sind nicht primär Gegenstand dieses neuen Bundesgesetzes.

7 Fazit

Der Bericht zeigt die kritischen Abhängigkeiten der sicherheits- und versorgungstechnischen Stabilität der Schweiz von Dienstleistungen und Fähigkeiten der Weltrauminfrastruktur auf. Diese Abhängigkeiten dürften in Zukunft weiter zunehmen. Im Zusammenspiel mit einer Diversifizierung von Akteuren im Raumfahrtbereich und von weltraumbasierten Dienstleistungen, sowie technologischen Trends, mehren sich die Cyberrisiken, die sich durch diese Abhängigkeiten für die Schweiz ergeben. Um sich angesichts der zunehmenden Verletzlichkeit besser zu schützen, kann die Schweiz folgende mögliche Massnahmen ergreifen:

1. Redundanzsysteme (weltraumgestützt oder terrestrisch) aufbauen und weltraumbasierte Anwendungen diversifizieren, um Auswirkungen eines Ausfalls oder einer Störung möglichst klein zu halten;
2. die gezielte Entwicklung eigener Fähigkeiten oder nationaler Infrastrukturen fördern, um Autonomie und Resilienz zu erhöhen.[115]

Der Bericht beleuchtet die Cyberrisiken, die sich durch die Abhängigkeiten von Weltrauminfrastruktur für die Schweiz ergeben. Die Weltrauminfrastruktur «Bodensegment – Datenverbindung – Weltraumsegment» weist in allen drei Segmenten zahlreiche und verschiedene Cyberrisiken auf. Die Schweiz hat mit einem vergleichsweise kleinen und wenig versorgungs- und sicherheitskritischen Bestand an Weltrauminfrastruktur nur begrenzte Möglichkeiten, im Betrieb der Weltrauminfrastruktur die Cybersicherheit zu stärken. Als Forschungs- und Entwicklungsstandort für Technologien, die in Weltrauminfrastrukturen eingesetzt werden, kann die Schweiz aber in der Entwicklung und Herstellung folgende mögliche Massnahmen ergreifen:

---

[110] SR 128.

[111] Z. B. Cloud Computing (Definition siehe Glossar). JAMES DALY, Why cloud and edge are launching the next space race, IBM, 2020, <https://www.ibm.com/blog/ibm-space-tech-cloud-edge-communication-breakthrough/>.

[112] STEFAN SOESANTO, Terra Calling: Defending and Securing the Space Economy, ETH Zürich, 2021, <https://doi.org/10.3929/ethz-b-000460220>.

[113] Weltraumpolitik 2023, 2023, S. 21. Es ist aber wichtig, bei der Ausarbeitung des nationalen Weltraumgesetzes die Prozesse der internationalen Koordination der Funkfrequenzen und Orbitalpositionen von Satelliten zu berücksichtigen.

[114] Das Projekt wird vom Eidgenössischen Departement für Wirtschaft, Bildung und Forschung (WBF) in Zusammenarbeit mit den anderen betroffenen Departementen erarbeitet. Der Bundesrat, Aktualisierung der Schweizer Weltraumpolitik und Erarbeitung einer nationalen Rechtsgrundlage für den Raumfahrtbereich, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87205.html> (besucht am 21. Juni 2022).

[115] Weltraumpolitik 2023, 2023, S. 17.

3. die Erhöhung der Cybersicherheit aller Software- und Hardwarekomponenten fördern durch die Anwendung von Security by Design Prinzipien in der Entwicklungsphase;
4. schweizweite Anreize oder Auflagen für private Hersteller und Betreiber der Weltrauminfrastruktur für Lieferketten- und Netzwerksicherheit setzen.[116]

Die Schweiz engagiert sich in multilateralen Gremien, internationalen Organisationen und Entwicklungsprogrammen zu Weltraumthemen und an der Schnittstelle Weltraum-Cybersicherheit. Sie ist als zuverlässige Akteurin anerkannt. Um ihre Interessen zu wahren und ihre Wettbewerbsfähigkeit und Relevanz zu steigern, ist die Schweiz auf die internationale Zusammenarbeit angewiesen. Um ihren Handlungsspielraum international auszuweiten, kann die Schweiz folgende mögliche Massnahmen ergreifen:

5. ihren Status in internationalen Organisationen als zuverlässige Akteurin wahren und sich weiterhin in internationalen Foren für eine friedliche, sichere und nachhaltige Nutzung des Weltraums einsetzen;[117]
6. die internationale Zusammenarbeit in Raumfahrtforschung und -projekten intensivieren durch eine stärkere Beteiligung an internationalen Technologieentwicklungs- und Forschungsprogrammen, um langfristig den Zugang zu Weltrauminfrastrukturen sicherzustellen, ihre Interessen zu wahren und ihre Resilienz zu erhöhen;[118]
7. sich für die Festigung und Weiterentwicklung ihrer Schlüsselkompetenzen in europäischen Entwicklungsprogrammen für Satellitenkommunikation frühzeitig positionieren und sich als zuverlässige Partnerin und Nutzerin der operationellen Systeme einbringen.[119]

Schliesslich wird die Schweiz betreffend die Rechtslage der Datenübermittlung im Weltraum folgende mögliche Massnahme ergreifen:

8. die zunehmend geführten juristischen Debatten in internationalen Foren über den rechtlichen Status der im Weltraum übertragenen und gespeicherten Daten im Auge behalten.[120]

Dieser Bericht hat acht mögliche Massnahmen aus den Leitfragen des Postulates abgeleitet. Die möglichen Massnahmen 1, 2, 5-8 sind verschiedenen strategischen Stossrichtungen, Zielen, Handlungsfeldern und Massnahmen strategischer Dokumente des Bundesrates zuzuordnen und konkretisieren bestimmte Handlungsfelder der Weltraumpolitik 2023.[121] Die konkrete Umsetzung erfolgt im Rahmen der bewilligten Kredite durch die Departemente in ihren jeweiligen Zuständigkeitsbereichen. Die Umsetzung wird durch die zuständigen Departemente überprüft. Über die Umsetzung der Weltraumpolitik 2023 erstatten das WBF, in Zusammenarbeit mit dem EDA, dem Eidgenössischen Departement des Innern (EDI), dem Eidgenössischen Finanzdepartement (EFD), dem Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) und dem VBS dem Bundesrat Bericht.[122]
Die möglichen Massnahmen 3 und 4 fallen in den Rahmen der NCS. Die Umsetzung der Strategie wird durch den Steuerungsausschuss der NCS geführt. Dieser verantwortet die Erstellung eines Umsetzungsplans und erstattet über seine Geschäftsstelle, welche durch das NCSC gestellt wird, dem Bundesrat und den Kantonen Bericht. Die Finanzierung der Umsetzungsarbeiten erfolgt grundsätzlich durch die zentralen Akteure selbst. Die Akteure des Bundes setzen dafür die Ressourcen ein, welche ihnen zur Umsetzung der vorgehenden beiden Cyberstrategien zugesprochen wurden.[123]

Diese Berichterstattung der sicherheits- und versorgungsrelevanten Cyberrisiken für die Schweiz im Gesamtsystem der Weltrauminfrastruktur ist den Massnahmen für das Ziel «Selbstbefähigung» der NCS zuzuordnen. Die Massnahme 3 «Bedrohungslage» erzielt eine Einschätzung zur Bedrohungslage, auf deren Grundlage Wirtschaft, Gesellschaft und Verwaltung ihre risikominimierenden Massnahmen möglichst kosteneffizient und zielgerichtet identifizieren und umsetzen können.[124] Cyberrisiken werden in der Bundesverwaltung in enger Zusammenarbeit mit den Kantonen und Wirtschaft und Gesellschaft fortlaufend beurteilt. Die Bedrohungslage soll dabei nicht nur grundlegende und breitenwirksame, sondern auch geschäfts- und prozessspezifische Bedrohungen aufzeigen.

---

[116] Nationale Cyberstrategie NCS, 2023, S. 20-21.

[117] U. a. Aussenpolitische Strategie 2020-2023, 2020, S. 15-20; der Sicherheitspolitische Bericht 2021, 2021, S. 10, 45; Strategie Digitalaussenpolitik 2021-2024, 2020, S. 9, 13; Strategie Rüstungskontrolle und Abrüstung 2022-2025, 2022, S. 30; Weltraumpolitik 2023, 2023.

[118] Weltraumpolitik 2023, 2023, S. 16-20.

[119] Die Sicherheitspolitik der Schweiz Bericht des Bundesrates (2021) BBl 2021 2895, S. 45; Weltraumpolitik 2023, 2023.

[120] STEFAN SOESANTO, Terra Calling: Defending and Securing the Space Economy, ETH Zürich, 2021, <https://doi.org/10.3929/ethz-b-000460220>.

[121] U. a. Aussenpolitische Strategie 2020-2023, 2020, S. 15-20; der Sicherheitspolitische Bericht 2021, 2021, S. 10, 45; Strategie Digitalaussenpolitik 2021-2024, 2020, S. 9, 13; Strategie Rüstungskontrolle und Abrüstung 2022-2025, 2022, S. 30; Weltraumpolitik 2023, 2023.

[122] Weltraumpolitik 2023, 2023, S. 2.

[123] Nationale Cyberstrategie NCS, 2023, S. 35.

[124] Nationale Cyberstrategie NCS, 2023, S. 16.

Dieser Bericht deckt sich auch – auf einem höheren Abstraktionsgrad – mit den Schwerpunkten der Massnahme 4 «Analyse von Trends, Risiken und Abhängigkeiten», z. B. das Monitoring von neuen Technologien oder der Analyse der Abhängigkeiten von Produkten und Zulieferern in der Schweiz.[125]

[125] Nationale Cyberstrategie NCS, 2023, S. 18.

8 Abkürzungsverzeichnis

API	Application Programming Interface
ARTES	Advanced Research in Telecommunications Systems
BABS	Bundesamt für Bevölkerungsschutz
BAFU	Bundesamt für Umwelt
BAKOM	Bundesamt für Kommunikation
CCSDS	Consultative Committee for Space Data Systems
CEPT	Conférence Européenne des Administrations des Postes et des Télécommunications European Conference of Postal and Telecommunications Administrations Europäische Konferenz der Verwaltungen für Post- und Fernmeldewesen
COTS	Commercial off-the-shelf
CSS	Centre for Security Studies
DG DEFIS	EU Generaldirektion Verteidigungsindustrie und Weltraum
DoSA	Defense of Space Assets
DSG	Datenschutzgesetz (SR 235.1)
T-DAB	Terrestrial Digital Audio Broadcasting
ETH	Eidgenössische Technische Hochschule
EU	Europäische Union
EGNOS	European Geostationary Navigation Overlay Service Regionales satellitenbasiertes Ergänzungssystem der EU
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EFD	Eidgenössisches Finanzdepartement
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ESA	European Space Agency
EUSPA	EU Agency for the Space Programme
EUMETSAT	European Organisation for the Exploitation of Meteorological Satellites Organisation für den Betrieb europäischer Wettersatelliten
EUTELSAT	European Telecommunications Satellite Organization Europäische Fernmeldesatellitenorganisation
ECC	Electronic Communications Committee
FAI	Fédération Aéronautique Internationale
FMG	Fernmeldegesetz (SR 784.10)
FDA	Anbieterinnen von Fernmeldediensten
Galileo	Globales Satellitennavigationssystem der EU
GPS	Global Positioning System
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GLONASS	Global Navigation Satellite System
GOVSATCOM	European Union Governmental Satellite Communications
ICG	International Committee on GNSS
IKAR	Interdepartementalen Koordinationsausschuss für Raumfahrtfragen
IKT	Informations- und Kommunikationstechnik
IMO	Internationale Seeschifffahrts-Organisation
IMSO	International Mobile Satellite Organization Internationale Organisation für mobile Satellitenkommunikation
IoT	Internet of Things
ISG	Informationssicherheitsgesetz (SR 128)

ITSO	International Telecommunications Satellite Organization Internationale Fernmeldesatellitenorganisation
ITU	International Telecommunication Union Internationale Fernmeldeunion
ITU-D	Telecommunication Development Sector Telekommunikation-Entwicklungssektor der ITU
ITU-R	Radiosektor der ITU
ITU-T	Standardisierungssektor der ITU
KI	Künstliche Intelligenz
LEO	Low-Earth Orbit
MIFR	Master International Frequency Register Internationale Frequenzreferenzdatei
NaFZ	Nationaler Frequenzzuweisungsplan
NCS	Nationale Cyberstrategie
NCSC	Nationales Zentrum für Cybersicherheit
NEO	Near-Earth Objects
NTP	Network Time Protocol
NIST	National Institute of Standards and Technology
NISV	Verordnung über den Schutz vor nichtionisierender Strahlung (SR 814.710)
OEWG	Open-Ended Working Group
PNT	Positioning, Navigation, Timing
PESCO	Permanent Structured Cooperation
PAROS	Prevention of an Arms Race in Outer Space
PPWT	Draft Treaty on the Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force against Outer Space Objects
PPP	Public-Private Partnerships
PRS	Public Regulated Service
QKD	Quantum Key Distribution
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SKI	Schutz kritischer Infrastrukturen
SPARTA	Space Attack Research & Tactic Analysis
SSA	Space Situational Awareness
SST	Space Surveillance and Tracking
SW	Space Weather
UNO	Vereinte Nationen
UN COPUOS	The UN Committee on the Peaceful Uses of Outer Space
UNGA	United Nations General Assembly
USG	Umweltschutzgesetz (SR 814.01)
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
WMO	World Meterological Organization

9 Glossar

Application Programming Interface (API)	Eine API stellt die Kommunikation zwischen zwei Programmen oder Systemen in Echtzeit her. Dabei werden Informationen zwischen einer Anwendung und einzelnen Programmteilen standardisiert ausgetauscht. Die Übergabe der Daten und Befehle erfolgt strukturiert nach einer definierten Syntax. Eine API ist die Vermittlungsschicht, die Datenübertragungen zwischen Systemen verarbeitet.[126]
Cloud Computing	Cloud Computing ist ein Modell zur Ermöglichung eines allgegenwärtigen und bedarfsgerechten Netzzugangs zu einem gemeinsamen Pool konfigurierbarer Rechenressourcen (z. B. Netze, Server, Speicher, Anwendungen und Dienste), die schnell und mit minimalem Verwaltungsaufwand oder Interaktion mit dem Dienstanbieter bereitgestellt und freigegeben werden können.[127]
Cyberbedrohung	Jeder Umstand oder jedes Ereignis mit dem Potenzial, einen Cybervorfall zu ermöglichen.[128]
Cyberkriminalität	Cyberkriminalität umfasst die Gesamtheit aller strafbaren Handlungen und Unterlassungen im Cyberraum. Unterschieden wird zwischen «Cybercrime» und «digitalisierter Kriminalität». «Cybercrime» bezeichnet Straftaten die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten und technische Ermittlungsarbeit auf Seiten der Strafverfolgungsbehörden erfordern. «Digitalisierte Kriminalität» bezeichnet Straftaten, die bisher überwiegend in der analogen Welt begangen worden sind. Aufgrund der zunehmenden Digitalisierung, werden diese klassischen Delikte vermehrt mit Hilfe von Informationstechnik verübt.[129]
Cybersicherheit	Anzustrebender Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert.[130]
Cybervorfall	Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist.[131]
Datenfluss	Datenfluss ist die Bewegung von Daten durch ein System, das aus Software, Hardware oder einer Kombination aus beidem besteht. Der Datenfluss wird häufig anhand eines Modells oder Diagramms definiert, in dem der gesamte Prozess der Datenbewegung von einer Komponente zur nächsten innerhalb eines Programms oder Systems abgebildet wird, wobei berücksichtigt wird, wie die Daten während des Prozesses ihre Form ändern.[132]
Dual-Use-Güter	Dual-Use-Güter, oder doppelt verwendbare Güter, sind Waren, Technologien und Software, die sowohl für zivile als auch für militärische Zwecke verwendet werden können.[133]
Halbleiter(chips)	Ein Halbleiter ist eine Substanz mit spezifischen elektrischen Eigenschaften, durch die sie sich als Grundlage für Computer und andere elektronische Geräte eignet. Es handelt sich in der Regel um ein festes chemisches Element oder eine Verbindung, die unter bestimmten Bedingungen Strom leitet, unter anderen jedoch nicht. Ein Halbleiter kontrolliert und steuert den Stromfluss in elektronischen Geräten und Anlagen. Daher ist er ein beliebter Bestandteil

[126] Was ist eine Application-Programming-Interface (API)?, Datacenter Insider, <https://www.datacenter-insider.de/was-ist-ein-application-programming-interface-api-a-735797/>; What is an API?, IBM, <https://www.ibm.com/topics/api>.

[127] MELL/GRANCE, NIST Special Publication 800-145 The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, NIST, 2011, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

[128] Nationale Cyberstrategie NCS, 2023.

[129] Ibid.

[130] Ibid.

[131] Ibid.

[132] What Does Dataflow Mean?, Techopedia, <https://www.techopedia.com/definition/6743/dataflow>.

[133] Güterkontrollgesetz (GKG, SR 946.202), <https://www.fedlex.admin.ch/eli/cc/1997/1697_1697_1697/de#art_3>.

	elektronischer Chips, die für Computerkomponenten und eine Vielzahl von elektronischen Geräten, einschliesslich Festkörperspeichern, hergestellt werden.[134]
Internet of Things (IoT)	Ein Netzwerk physischer Objekte (Dinge), die mit Sensoren, Software und anderer Technologie ausgestattet sind, um diese mit anderen Geräten und Systemen über das Internet zu vernetzen, sodass zwischen den Objekten Daten ausgetauscht werden können.[135]
Jamming	Unter Jamming, oder Signalstörung, versteht man die Unterbrechung der Verbindung zwischen einem Gerät und seinem Zugangspunkt in einer drahtlosen Verbindung. Geräte in einem drahtlosen Netzwerk senden und empfangen Informationen mithilfe von Datenpaketen auf einer bestimmten Frequenz. Beim Stören von Signalen wird ein Störsender verwendet, um "Rauschen" zu senden, das das Frequenzband stört, auf dem drahtlose Geräte Datenpakete austauschen.[136]
Kaskadeneffekte	Sind technische Systeme oder Bauteile in Reihe geschaltet (in der Elektronik spricht man von Kaskadierung) oder in schwer überschaubarer Weise miteinander verknüpft, entstehen Kaskadenrisiken. Es kann dann zu unerwünschten oder sogar katastrophalen Kaskadeneffekten kommen, die hinsichtlich ihrer Auswirkungen in einem Missverhältnis zum oft banalen Auslöser („Trigger“) stehen.
Kritische Infrastruktur	Als kritische Infrastrukturen werden Prozesse, Systeme und Einrichtungen bezeichnet, die für das Funktionieren der Wirtschaft beziehungsweise für die Lebensgrundlagen der Bevölkerung essenziell sind.[137]
Künstliche Intelligenz (KI)	Künstliche Intelligenz ist der Überbegriff für Anwendungen, bei denen Maschinen menschenähnliche Intelligenzleistungen erbringen. Darunter fallen das maschinelle Lernen (Machine Learning), das Verarbeiten natürlicher Sprache (NLP – Natural Language Processing) und Deep Learning, ein Teilgebiet von maschinellem Lernen, welches sich auf künstliche neuronale Netze und grosse Datenmengen fokussiert.[138]
Maschinelles Lernen	Maschinelles Lernen ist ein Teilbereich der künstlichen Intelligenz. Der Schwerpunkt liegt dabei auf dem Trainieren von Computern, um aus Daten und Erfahrungen zu lernen und sich stets zu verbessern – anstatt explizit dafür programmiert zu werden. Beim maschinellen Lernen werden Algorithmen darauf trainiert, Muster und Korrelationen in grossen Datensätzen zu finden und auf Basis dieser Analyse die besten Entscheidungen und Vorhersagen zu treffen. Anwendungen für maschinelles Lernen verbessern sich mit ihrer Nutzung und werden umso genauer, je mehr Daten sie zur Verfügung haben.[139]
Network Time Protocol	Network Time Protocol (NTP) ist ein Protokoll zur Synchronisierung von Uhren in Computersystemen.[140]
Patches, Updates, Upgrades	Patches sind kleine Softwareupdates, die ein oder mehrere Probleme einer Anwendung beheben. Typischerweise werden Patches von Herstellern oder Programmierern zur Verfügung gestellt, um eine Unschönheit oder einen Fehler einer Anwendung zu beheben. Patches werden jeweils zeitnah zu aufgetretenen Problemen erstellt. Das Einspielen oder Aktivieren eines Patches ge-

[134] ANDREW ZOLA, Halbleiter, ComputerWeekly.de, <https://www.computerweekly.com/de/definition/Halbleiter>. (besucht am 20. April 2023)

[135] Was ist das IoT?, Oracle, <https://www.oracle.com/ch-de/internet-of-things/what-is-iot/>. (besucht am 20. April 2023)

[136] What is Signal Jamming and What Can You Do About It?, Make Use Of, 2022, <https://www.makeuseof.com/what-is-signal-jamming/>.

[137] Nationale Strategie zum Schutz kritischer Infrastrukturen, 2023, BBl 2023, 1659 ff., S. 3.

[138] Was ist künstliche Intelligenz?, SAP, <https://news.sap.com/germany/2018/03/was-ist-kuenstliche-intelligenz/>. (besucht am 10. April 2023); Was ist Deep Learning?, datasolut, <https://datasolut.com/was-ist-deep-learning/#:~:text=Deep%20Learning%20(tiefes%20Lernen)%20ist,und%20Entscheidungen%20genauer%20zu%20t%C3%A4tigen.>.

[139] Was ist maschinelles Lernen?, SAP, <https://www.sap.com/swiss/insights/what-is-machine-learning.html#:~:text=Maschinelles%20Lernen%20ist%20die%20Verschmelzung,f%C3%BCr%20die%20Analyse%20zu%20erstellen.>.

[140] Network Time Protocol (NTP): Definiton und Funktionsweise, IONOS, <https://www.ionos.de/digitalguide/server/knowhow/network-time-protocol-ntp/>.

	schieht meistens im laufenden Betrieb und ohne eigentliche Wahrnehmung durch die Anwender. Beinhaltet ein Patch auch neue Funktionen oder z. B. eine Anpassung eines Layouts, spricht man von Updates. Ein Update bedingt meistens auch einen Unterbruch für dessen Einspielung. Im Gegensatz zu Updates beinhalten Upgrades wesentlichen funktionale Erweiterungen und gegebenenfalls neue Funktionsbereiche.[141]
Penetrationstest	Ein Penetrationstest, kurz Pentest, beschreibt ein Verfahren, um die aktuelle Sicherheit einer IT-Landschaft oder einer (Web-)Anwendung festzustellen. Er gilt als Sicherheitscheck von IT-Systemen jeder Grössenordnung und ist besonders für Unternehmen relevant. Für diese Sicherheitsüberprüfung bedient sich der Pentester den Mitteln und Methoden, die ein Hacker anwenden würde, um in das System einzudringen – es zu penetrieren. Mithilfe des Pentests wird festgestellt, wie empfindlich ein System auf derartige Angriffe reagiert.[142]
Positioning, Navigation, Timing (PNT)	Positionierung, oder Positionsdaten, sind die Bestimmung einer Position und allenfalls Orientierung in einem räumlichen Bezugsrahmen mit einer bekannten Genauigkeit. Navigation ist die Bestimmung von aktueller und gewünschter Position und Orientierung, Anbringen von Korrekturen an Kurs und Geschwindigkeit zur Erreichung einer Destination. Timing, auch Zeitsignal, ist die Synchronisation von Uhren bezüglich einer Standardzeit (zum Beispiel UTC) mit einer bekannten Genauigkeit.[143]
Quantum Key Distribution	Quantum Key Distribution, oder Quantenschlüsselaustausch, ist ein bekanntes und bereits praktisch eingesetztes Verfahren der Quantenkryptographie. Unter Nutzung quantenmechanischer Effekte können zwei Kommunikationspartner einen für die symmetrische Verschlüsselung einsetzbaren Schlüssel abhörsicher austauschen. Die Sicherheit des Schlüsselaustauschs basiert nicht mehr auf mathematischen Algorithmen und Annahmen zur Rechenleistung von Computern, sondern auf physikalischen Gesetzen der Quantenmechanik. Der Quantenschlüsselaustausch wurde bereits praktisch eingesetzt. Die überbrückbaren Distanzen sind jedoch begrenzt.[144]
Resilienz	Die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und das ordnungsgemässe Funktionieren zu erhalten oder dieses möglichst rasch und vollständig wiederzuerlangen.[145]
Satelliten- Erdumlaufbahn	Satelliten werden in der Regel nach ihrer Erdumlaufbahn (Entfernung von der Erdoberfläche) klassifiziert, die sich direkt auf ihre Empfangsleistung und die Geschwindigkeit auswirkt, mit der sie sich um den Planeten bewegen. Grundlegende Erdumlaufbahnen und die jeweilige Nutzung von Satelliten: - Low Earth Orbit (LEO-)Satelliten bewegen sich in einer Höhe von etwa 160-1.500 km über der Erdoberfläche. Sie haben eine kurze Umlaufzeit von 90 bis 120 Minuten. Sie eignen sich besonders gut für Fernerkundung, hochaufgelöster Erdbeobachtung und Forschung, da Daten relativ schnell erfasst und übertragen werden können. - Die mittlere Erdumlaufbahn (MEO) liegt zwischen der niedrigen Erdumlaufbahn und der geostationären Umlaufbahn und befindet sich in der Regel in einer Höhe von 5’000 bis 20’000 km. Positionierungs- und Navigationsdienste wie GPS nutzen generell MEO-Satelliten.

[141] Patch, Update, Upgrade. Aspectra. <https://www.aspectra.ch/blog/patch-update-upgrade--b512>; <https://odion.com/?faqs=was-ist-der-unterschied-zwischen-update-upgrade-release-und-change-request#:~:text=Updates%20sind%20technische%20Modifikationen%2C%20Verbesserungen,neue%20Funktionsbereiche.>.

[142] Penetrationstest – Definition. IT-Service.Network. <https://it-service.network/it-lexikon/penetrationstest>.

[143] Bundesamt für Landestopografie swisstopo. Swisstopo Kolloquium Positioning, Navigation, Timing (PNT). <https://www.swisstopo.admin.ch/content/events/de/swisstopo-internet/events2022/colloquium-21-22/20220114/_jcr_content/contentPar/downloadlist/downloadItems/272_1642173963101.download/220114_Kolloquium_PNT_alle.pdf>.

[144] Was ist Quantenschlüsselaustausch?, Security Insider, <https://www.security-insider.de/was-ist-quantenschluesselaustausch-a-5fd80c11f9b676caa394bcac7c73feb4/>.

[145] Nationale Cyberstrategie NCS, 2023.

- Satelliten in der geostationären Erdumlaufbahn (GEO) befinden sich 35’786 km über der Erdoberfläche, genau über dem Äquator. Objekte in GEO erscheinen vom Boden aus unbeweglich, da ihre Umlaufzeit identisch zur Erdrotation ist. Eine terrestrische Antenne kann immer auf dasselbe Gerät im Weltraum ausgerichtet werden, weshalb dieser Satellitentyp für durchgehend verfügbare Kommunikationsdienste wie TV und Telefonie oder Meteorologie eingesetzt werden. Ein Nachteil von GEO-Satelliten ist die längere Signalverzögerung der Echtzeitkommunikation, die durch die grosse Entfernung zur Erde verursacht wird.[146]

Schwachstelle	Eine Schwachstelle in der Informationstechnologie (IT) ist ein Fehler im Code oder Design, der eine potenzielle Sicherheitslücke für einen Endpunkt oder ein Netzwerk darstellt. Schwachstellen schaffen mögliche Angriffsvektoren, durch die Angreifende Code ausführen oder auf den Speicher eines Zielsystems zugreifen könnten.[147]
Security by Design	Security by Design ist ein in der Hard- und Softwareentwicklung angewandtes Designkonzept. Die Sicherheit der Hard- oder Software wird bereits im Entwicklungsprozess berücksichtigt und in den kompletten Lebenszyklus eines Produkts integriert. Zu den Designkriterien zählen beispielsweise die Minimierung der Angriffsfläche, der Einsatz von Verschlüsselung und Authentifizierung und die Isolation sicherheitsrelevanter Bereiche. Die Sicherheit wird kontinuierlich getestet.[148]
Service public	Service public umfasst die Grundversorgung mit Infrastrukturgütern und -dienstleistungen, welche für alle Bevölkerungsschichten und Regionen des Landes zu gleichen Bedingungen in guter Qualität und zu angemessenen Preisen zur Verfügung stehen sollen.[149]
Software-definierte Satelliten	Im Allgemeinen bedeutet «softwaredefiniert», dass herkömmliche Hardwarekomponenten durch Software ersetzt werden. Das übergreifende Software-Defined Networking ist ein Netzkonzept, das Hard- und Software entkoppelt. Das heisst, die Steuerung des Netzwerks ist von der Hardware, welche die eigentlichen Datenweiterleitung durchführt, getrennt. Die Möglichkeit, den Satelliten neu zu konfigurieren, bedeutet, dass die Mission während seiner gesamten Lebensdauer variieren und an veränderte Anforderungen angepasst werden kann.[150]
Space Situational Awareness	Space Situational Awareness (SSA) bezieht sich auf die Kenntnis der Weltraumumgebung, einschliesslich Standort und Funktion von Weltraumgegenständen und Weltraumwetterphänomenen.[151]
Spoofing	Der Begriff Spoofing (Täuschung, Verschleierung, Manipulation) bezeichnet eine Angriffstechnik, bei der Cyberkriminelle in Computer oder Netzwerke eindringen, indem sie eine vertrauenswürdige Identität vortäuschen.[152]
Up-Link/Down-Link	In der Satellitentelekommunikation ist ein Downlink die Verbindung von einem Satelliten nach zu einer oder mehreren Bodenstationen oder Empfängern. Ein Uplink ist die Verbindung von einer Bodenstation zu einem Satelliten.[153]

[146] Types of Satellites: Different Orbits & Real-World Uses, EOS Data Analytics, <https://eos.com/blog/types-of-satellites/>.

[147] Vulnerability (information technology), WhatIs.com, <https://www.techtarget.com/whatis/definition/vulnerability>.

[148] Was ist Security by Design?, Security Insider, <https://www.security-insider.de/was-ist-security-by-design-a-1071181/>.

[149] Ein guter Service public - das Markenzeichen der Schweiz, Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK, <https://www.uvek.admin.ch/uvek/de/home/uvek/bundesnahe-betriebe/guter-service-public.html>.

[150] Was ist Software-Defined Networking (SND)?, IP Insider, <https://www.ip-insider.de/was-ist-software-defined-networking-sdn-a-657442/>; Software Defined Satellites, Businesscom, <https://www.bcsatellite.net/blog/software-designed-satellites/#:~:text=The%20term%20Software%20Defined%20Satellite,adjusted%20based%20on%20changing%20demands.>.

[151] Space Situational Awarenes (SSA), SatCen, <https://www.satcen.europa.eu/page/ssa>.

[152] Spoofing – Definition, IT-Security.Network, <https://it-service.network/it-lexikon/spoofing>.

[153] What is downlink and uplink?, TechTarget, <https://www.techtarget.com/searchmobilecomputing/definition/downlink-and-uplink#:~:text=In%20satellite%20telecommunication%2C%20a%20downlink,station%20up%20to%20a%20satellite.>.