



Satelliten-Abwehrsystem

Weltraumbasierte Systeme sind für die Durchführung von Land-, See- und Luftoperationen von essenzieller Bedeutung. Moderne Satelliten beobachten Operationsräume und Hinterland unabhängig von Tageszeit oder Wetter und bieten omnipräsente Kommunikation mit hoher Bandbreite und geringen Latenzzeiten. Diese Kritikalität für Logistik, Kommunikation und militärische Operationen ist seit dem Ukraine Konflikt in der breiten Öffentlichkeit angekommen.

Problemdarstellung: *Trotz ihrer Bedeutung sind Satellitensysteme jedoch eine relativ verwundbare Infrastruktur, und Möglichkeiten zur Bekämpfung einzelner Objekte bis hin zur Unbrauchbarmachung ganzer Konstellationen und Orbits stehen einer Reihe Nationen zur Verfügung.*

Was nun?: *Für die Sicherstellung zukünftiger Operationen braucht es daher eine systematische Risikobetrachtung der Ressource Weltraum, passende Schutz- und Resilienzkonzepte für bestehende und zukünftige Systeme, wie auch die Entwicklung von alternativen Fähigkeiten, um Kommunikation nach einem katastrophalen Vorfall ohne Weltraum-basierte Systeme sicherstellen zu können.*

Die Bedeutung des Weltraums

Seit Sputnik 1957 die Erde mit einem periodischen Piepen umkreiste, sind Satelliten zu einem essenziellen Element unseres täglichen Lebens geworden. Mehr als 8.000 aktive Satelliten stellen Dienstleistungen an Militär, Regierungen, Unternehmen und Privatpersonen zur Verfügung. Logistik, Luft- und Seefahrt, sowie die Landwirtschaft, nutzen zentimetergenaue Positionsbestimmungen. Satelliten beobachten Wetter und Umwelt und sind der führende Verbreitungsweg für Fernsehinhalte weltweit. Satelliten vermitteln Datenverbindungen an Flugzeuge und Schiffe. Sie bringen Telefonie und Internet nicht nur in entlegene Gebiete, sondern auch quer durch Deutschland.

Die Ressource Weltraum ist auch für Militäroperationen unverzichtbar geworden. Aufklärung und Spionage aus dem Weltall schaffen strategische Vorteile, gleichzeitig bringt eine permanente Überwachung – mit Hilfe von Synthetic Aperture Radar (SAR) auch bei Nacht und durch Wolkendecken hindurch – neben neuen Möglichkeiten auch neue strategische Herausforderungen für offensive wie defensive Missionen, wie aktuell in der Ukraine zu beobachten. Ohne Satelliten wäre es schlicht nicht möglich, unbemannte Systeme weltweit oder außerhalb gesicherten Territoriums oder über eigene Landesgrenzen hinweg effektiv einzusetzen. Weltrauminfrastruktur wird damit auch Angriffsziel, wie Hacks des KA-SATS zum Auftakt des Ukrainekriegs und russische Drohungen gegen Starlink deutlich gemacht haben.

Technischer Aufriss der Komponenten eines Satellitensystems

Um Kommunikation oder Beobachtungen aus dem Weltraum bereitzustellen, benötigt es ein Portfolio an Infrastruktur, welches im Folgenden kurz angerissen wird.

LEO, MEO, GEO – Die Höhe bestimmt die Anwendungen

Fußball-Endspiel, Elfmeterschießen nach Verlängerung, der entscheidende Ball. Während der Stürmer auf dem heimischen Fernseher noch innehält, bricht bei den Nachbarn bereits Jubel aus, bevor nun auch in den eigenen vier Wänden der Ball

unhaltbar im Netz landet. Diese Verzögerung ist dem Weltraum geschuldet, genauer gesagt den mehr als 70.000 km, die das Signal im Satellitenfernsehen zusätzlich zurücklegen musste. Während kleine Latenzzeiten in TV und Radio-Rundfunk nicht von großer Bedeutung sind, sind gerade bei Echtzeitanwendungen solche Signalverzögerungen nicht tragbar. Um schnelles Internet zu realisieren oder eine Drohne mit Hilfe von Bild und Telemetriedaten sicher ins Ziel zu steuern, muss die Verzögerung so kurz wie möglich sein und der Satellit damit so tief über seinen Nutzern fliegen wie nötig.

Es gibt wesentliche Unterschiede zwischen einer Bewegung auf der Erde (z. B. eines Flugzeugs) und eines Objektes im Weltraum. Die Geschwindigkeit eines Flugzeugs ist unabhängig von der Flugbahn: Ein Sportflugzeug ist auf dem gleichen Kurs und in gleicher Höhe wesentlich langsamer unterwegs als typischerweise ein Jet, während im Weltraum alle Objekte in einem bestimmten Orbit die gleiche Geschwindigkeit haben müssen, bei der sich Zentrifugal- und Gravitationskraft die Waage halten. Auf 800 km Höhe bedeutet dies eine Geschwindigkeit von 7,5 km pro Sekunde, der 30-fachen Geschwindigkeit eines Passagierflugzeugs. Je höher der Satellit über der Erde ist, desto geringer ist die Gravitation, und die notwendige Umlaufgeschwindigkeit sinkt.

Ferner benötigen Satelliten im Gegensatz zu Objekten auf der Erde keinen Erhaltungsimpuls. Einmal in den Orbit gebracht, verbleibt der Satellit ohne weitere Energiezufuhr auf seiner Flugbahn. Jedoch ist der Weltraum nicht leer. Minimale Atmosphäre in niedrigen Orbits bremst Satelliten ab, sodass diese Treibstoff mitführen, um durch Flugbahnkorrekturen ihren Orbit zu halten.

Auf welcher Höhe ein Satellit installiert wird, hängt daher vor allem von der Verwendung und Anforderung der Nutzer ab. Objekte im geosynchronen Orbit (GEO) bewegen sich genauso schnell wie die Erde, Satelliten auf 0 Grad „schweben“ über einem fixen Punkt am Äquator und können aus 35,786 km Entfernung große Teile der Erdoberfläche beobachten und erreichen. Ein einzelner Fernsehsatellit im GEO kann damit die z.B. Nord- und Südamerika bis einschließlich Hawaii abdecken, während aufgrund der stationären Position die Nutzer eine einmal ausgerichtete Antenne nicht verändern müssen. Der lange Übertragungsweg bringt allerdings Verzögerungen mit sich, die für eine Vielzahl von Applikationen nicht akzeptabel sind. Satelliten auf niedrigen Flughöhen (Low Earth Orbits – oder kurz LEO) erreichen dagegen Latenzzeiten im 25- bis 100-ms-Bereich und hohe Datenraten. Orbitbedingt bewegen sie sich dadurch aber deutlich schneller als die Erde. Ein Iridium-Kommunikationssatellit umkreist die Erde alle 100 Minuten und ist dadurch nur ca. 7 Minuten in Sichtweite eines Empfängers. Dies macht große Stückzahlen nötig, die auf dem gleichen Orbit die Erde umkreisen, Verbindungen an einen Nachbarn übergeben und Daten untereinander bis zur nächsten Bodenstation weiterreichen, um dauerhaft Kommunikation (oder Überwachung) eines Ortes oder einer Region sicherzustellen. Durch ihre niedrige Flughöhe ist es aber einfach, mit geringem Energiebedarf Signale an den Satelliten zu senden. Während das Fernsehstudio eine große Satellitenschüssel und viel Sendeleistung braucht, können Mobiltelefone und bereits kleine Sensoren Verbindungen in den LEO aufbauen. Ein Mittelweg der verschiedenen Orbits ist der Medium Earth Orbit (MEO) auf mehreren Tausend Kilometern Höhe, ein Kompromiss zwischen Latenz, Sendeleistung, Abdeckung und damit nötiger Anzahl an Satelliten. Alle globalen Satelliten-Positionierungssysteme befinden sich im MEO. Die Anwendung des Satelliten bestimmt den Orbit, und aufgrund ihrer physikalischen Charakteristika lassen sich diese untereinander nicht substituieren.

Während Satelliten und die Transportkosten ins All vergleichsweise teuer waren, sanken durch die Fließbandfertigung und Miniaturisierung der Satelliten sowie der Wiederverwendbarkeit des SpaceX Trägersystems die Kosten so weit, dass große Konstellationen ökonomisch tragfähig wurden. So umfasst die LEO Starlink-Konstellation aktuell mehr als 5.000 Satelliten (mit weiteren 15.000 genehmigten), wobei die Kosten eines Starlinks mehrere Größenordnungen kleiner als die eines GEOs liegen.

Das Ökosystem Satellit

Die Bereitstellung eines Satelliten macht den Betrieb eines ganzen Ökosystems nötig. Bodenstationen übertragen und empfangen Nutzsignale zum und vom Satelliten, ferner überwachen Kontrollstationen Flugbahn und Betrieb des Systems und nehmen Korrekturen vor. Hierfür stehen spezielle Kommunikations- und Kontrollkanäle (TT&C) für Telemetrie und Steuerung zur Verfügung.

Die Bereitstellung eines Satelliten macht den Betrieb eines ganzen Ökosystems nötig. Bodenstationen übertragen und empfangen Nutzsignale zum und vom Satelliten, ferner überwachen Kontrollstationen Flugbahn und Betrieb des Systems und nehmen Korrekturen vor. Hierfür stehen spezielle Kommunikations- und Kontrollkanäle (TT&C) für Telemetrie und Steuerung zur Verfügung.

Verwundbarkeiten und Risikoanalyse

Sicherheitsmaßnahmen kosten Geld, aufgrund von fehlenden Anreizen sowie einer als gering empfundenen Bedrohungslage wurden im kommerziellen Satellitengeschäft in der Vergangenheit nur minimale Sicherheitsvorkehrungen getroffen. Exemplarisch sind Aussagen zu nennen, dass eine Verschlüsselung die verfügbare Bandbreite drastisch reduzieren würde [9]. Angriffe auf das Ökosystem Satellit lassen sich in vier Klassen aufteilen: kinetische Angriffe, nichtkinetische physische Angriffe, Cyber-Angriffe sowie Angriffe auf die Kommunikationsverbindungen.

Kommunikationsverbindungen

Mögliches Ziel von Angreifern sind sowohl die Funkstrecken zwischen Bodenstation und Satellit (Uplink) für Kontrollsignale und Nutzdaten, die Ausstrahlung von Daten vom Satelliten zu den Empfängern (Downlink), als auch Verbindungen innerhalb von Satelliten-Konstellationen. Zum einen können Angreifer Signale passiv mitlesen, zum anderen auch direkt in Uplink oder Downlink eingreifen, um die Verbindung zu stören (Jamming) oder manipulierte Daten einzuspielen (Spoofing). Obwohl Jamming ein trivialer Angriff ist, ist die Verteidigung je nach Ausführung verhältnismäßig aufwendig. Angriffe lassen sich vom Boden, aus dem Weltall, oder der Luft z. B. von einem Flugzeug oder Drohne ausführen, wenn der Angreifer im Empfangsbereich oder Abstrahlungswinkel des Satelliten ist. Insbesondere beim Downlink Jamming lässt sich der Ort der Störung gut bestimmen und angreifen, ein gezieltes Uplink Jamming ist schwieriger zu lokalisieren. Zwar lassen sich Störsignale technisch mit Richtantennen und speziellen Coding-Schemata dämpfen und filtern, diese sind allerdings in kommerziellen Systemen eher nicht zu finden, u.a. weil größtmögliche Abdeckung für die Kunden erreicht werden soll. Beim Spoofing wird dem System ein decodierbares, aber falsches Signal untergeschoben, z. B. um Steuerungskommandos auszulösen. Deutlich komplexer in der Realisierung, erfordert dieser Angriff aber auch andere erweiterte Maßnahmen wie z. B. die Authentifizierung von Signalen und damit den Austausch von Schlüsselmaterial.

Auch wenn hier mittlerweile ein Umdenken in der Industrie eingesetzt hat, verhindern lange Produktzyklen schnelle Veränderungen. Verschiedene Studien zeigen, dass Sprache und Daten z. B. aus Iridium- oder maritimen VSAT-Systemen [16] mit Standardkomponenten und wenigen Hundert Euro Budget mitgeschnitten werden können, und dass Endnutzer von Satellitenkommunikation oft keine eigene Transportsicherung nutzen. Auch die Technik für das Stören von Satellitenkommunikations- und GPS-Signalen ist mittlerweile breit und preisgünstig verfügbar [1] und die gezielte „Umpositionierung“ durch GPS Spoofing wird in der Praxis regelmäßig beobachtet [14]. Die oftmals unzureichende Sicherheit von kommerziellen Satellitensystemen betrifft auch den militärischen Bereich, da regelmäßig auf kommerzielle Bandbreite zurückgegriffen wird. So wurden z. B. 60% der militärischen Kommunikation in Afghanistan und 84% im Irakkrieg über kommerzielle Systeme abgewickelt [5, 17], wobei im Irak, Afghanistan und Bosnien Gegner Downlink-Signale auswerteten, um bevorstehenden Operationen auszuweichen [12].

Cyber-Angriffe

Der Bordcomputer eines Satelliten überwacht und steuert Sensorik, Kommunikationstechnik und Flugbahn und kann von der Kontrollstation instruiert werden. Über diesen Kanal oder mögliche Verwundbarkeiten in der Zugriffskontrolle könnte ein Angreifer die Steuerung eines Satelliten übernehmen und im schlimmsten Fall den Wiedereintritt und Verlust des Systems auslösen. So wurde 1998 der US-deutsche ROSAT beschädigt, als seine Instrumente direkt in die Sonne gedreht wurden [6], 2007 und 2008 erlangten Angreifer Kontrolle über die Terra EOS-Satelliten der NASA.

Nichtkinetische Angriffe

Satelliten können temporär oder dauerhaft mit nichtkinetischen Mitteln beeinträchtigt werden. Zum einen kann die Sensorik – permanent oder temporär – geblendet werden, um zu verhindern, dass während des Überfluges eines Zielgebiets optische Beobachtungen gemacht werden. Hierbei eignen sich Laser, die am Grund, in Flugzeugen oder im Weltraum stationiert werden können. Diese erfordern allerdings genaues Wissen über die Funktionsweise der Sensorik, die verwendeten Spektren sowie geeignete Laser in diesen Frequenzbereichen. Erste Experimente z. B. von China zu Bodenbasierten Störlasern reichen bis 2006 zurück, während Berichten in diesem Jahr zufolge eine chinesische Anti-Satelliten-Laserinstallation realisiert werden konnte [10].

Neben dem Blenden der Sensorik können Energiewaffen ebenfalls die Bordelektronik stören, das System überhitzen oder die Solarzellen beschädigen, und so vorübergehend oder dauerhaft einen Ausfall herbeiführen. Dieser Effekt ließe sich mit Hilfe von Lasern oder Mikrowellen im Megawatt-Bereich innerhalb von wenigen Sekunden bei LEO-Satelliten realisieren [3].

Kinetische Angriffe

Sowohl Bodenstationen als auch Satelliten selbst sind für kinetische Angriffe verwundbar. Während Bodenstationen als große, fixe Installationen leichte Ziele darstellen, können auch kleine, mobile Endgeräte durch ihre Uplinks lokalisiert und angegriffen werden.

Für die Zerstörung von Satelliten im Orbit existieren eine Reihe von Technologien für kinetische Anti-Satellite (ASAT) Waffensysteme: Erstens mittels gezieltem Beschuss mit Projektilen – entweder per Rakete vom Boden oder Co-Orbital von einem ASAT-System im Orbit. Zweitens durch Anbringen einer Sprengladung oder Detonation eines Satelliten in direkter Umgebung des Ziels. Drittens könnte ein feindlicher Satellit mit Hilfe eines Greifarms das Ziel aus der Umlaufbahn schieben oder zum Absturz bringen. Viertens mittels Einbringen von Material auf Kollisionskurs in die Umlaufbahn des Zieles, welches durch die große Menge Weltraumschrott in der Umlaufbahn schwer nachzuweisen und zu attributieren wäre.

Während die USA die Fähigkeit für Boden-basierte kinetische ASATs seit den 1980ern besitzen, haben seit den frühen 2000ern eine Reihe Nationen in die Entwicklung von ASAT investiert. Besondere Aufmerksamkeit erlangte der Test einer chinesischen ASAT-Rakete 2007, die schätzungsweise mehr als 100.000 Trümmerteile und einen substanziellen Prozentsatz des Weltraummülls im LEO verursachte, wie auch die erfolgreiche Demonstration eines Abschleppmaneuvers durch den Shijian-21-Satelliten im GEO [15]. Seit 2010 gab es mindestens zwei Dutzend Tests verschiedener Systeme, wobei besonders Russland und China diverse Kapazitäten entwickelt haben, und Ambitionen bzw. erste Ansätze von Indien und Iran verfolgt werden [7]. Selbst Nationen ohne Zugang zu gezielten, kinetischen ASAT können Satelliten zerstören, indem mit Hilfe von ballistischen Raketen Störkörper in die grobe Flugbahn eines Satelliten ausgebracht werden, allerdings mit erheblichen Kollateralschäden.

Was ist der Plan B?

Durch die Erd- und Weltraum-gebundene Beobachtung von Satellitenstarts und Flugbahnen im Orbit ist die Position von Satelliten bekannt, und in Ermangelung von Geländedeckung können diese verfolgt und angegriffen werden. Wegen dieser generellen Verwundbarkeit und der Abhängigkeit von Gesellschaften und Schlüsselnutzern stellt sich dringend die Frage nach alternativer Infrastruktur im Falle eines lokal begrenzten oder großflächigen Ausfalls der Ressource Weltraum. Welche Optionen zur Verfügung stehen, hängt auch von Art und Umfang der Intervention ab. Hier sollen im Folgenden drei Szenarien exemplarisch beleuchtet werden: die gezielte (Zer-)Störung von einzelnen Satelliten, ein Komplettausfall der Satelliteninfrastruktur sowie die Zerstörung und Unbrauchbarmachung von Orbits selbst.

Einzelne Satelliten

Es existieren verschiedene Technologien von Anti-Satellitenwaffen, um einzelne Systeme durch kinetische, nichtkinetische oder Cyberangriffe temporär oder permanent zu zerstören, bzw. die Kommunikationsverbindungen von Satelliten zu beeinflussen. Während gegen z. B. Energiewaffen ein gewisser Schutz durch Systemhärtung und Schilde erreicht werden kann, finden diese in den meisten Satellitensystemen aufgrund von Gewicht und damit Startkosten sowie eines nicht wahrgenommenen Risikos keine Verwendung. Aufgrund der hohen Geschwindigkeiten im Orbit und der damit verbundenen kinetischen Energie ist die Verteidigung gegen Projektil- und Explosivstoffe dagegen nicht kosteneffizient umzusetzen, und auch gegen sogenannte Orbit Threats – feindliche Systeme, die z. B. mit Hilfe eines Roboterarms einen Satelliten aus der Flugbahn oder zum Absturz bringen – existieren zum aktuellen Zeitpunkt keine effektiven, marktreifen Verteidigungsmaßnahmen.

Einen besseren Schutz und abschreckende Wirkung hat wahrscheinlich eher das ökonomische Missverhältnis zwischen Kosten eines ASAT-Systems und eines Satelliten kombiniert mit schnellen Wiederherstellungszeiten, was allerdings nur bei massenproduzierten Systemen zum Tragen kommt. So setzt eine Falcon 9 der amerikanischen SpaceX pro Flug routinemäßig fünf Dutzend Starlink-Satelliten im Orbit aus, während die neueren Trägersystementwicklungen von SpaceX die Kapazitäten bei stetig fallenden Startkosten noch deutlich erhöhen werden. Die Bekämpfung von einzelnen Satelliten einer großen Konstellation durch kostspielige kinetische ASAT ist damit wenig aussichtsreich, wenn die Fähigkeiten verloren gegangener Satelliten durch andere kompensiert und Verluste schnell ausgeglichen werden können – eine ähnliche Asymmetrie und Paradigmenverschiebung, wie sie sich auch gerade an verschiedenen Aspekten im Ukrainekrieg beobachten lässt.

Diese Konzeption ist jedoch aktuell (systemisch) die Ausnahme, und die meisten bestehenden Systeme wären durch die Vernichtung einzelner Satelliten deutlich beeinträchtigt. Diese Abhängigkeit und Verwundbarkeit wäre für die Vereinigten Staaten und europäische NATO-Partner höher als für andere Akteure in der Welt, und würde die Operationsfähigkeit bzw. Überlegenheit in entfernten Gegenden – z. B. im südostasiatischen Raum – deutlich mindern. Aus derartigen Überlegungen

verfolgt z. B. China in der letzten Dekade eine gezielte Innovationsagenda mit dem Ziel der Weltraum-Überlegenheit, um Gegnern die Möglichkeit von Weltraum-basierter Informationsgewinnung und Kommunikation zu verweigern. In diesem Kontext sollten technologische Entwicklungen wie bodengeschützte ASAT-Raketen (2007), Präzisionsrendezvous im Orbit (2010, 2013), Test von Roboterarmen (2016) und Hochleistungs-Laserstationen (2022) sowie aktuelle Forschung zu SAR Jamming im Zusammenhang mit dem Kapazitätsaufbau in anderen gesehen werden.

Komplettausfall der Satelliteninfrastruktur

Neben der Störung einzelner Systeme mit begrenzten geografischen Auswirkungen sollte aus Verteidigersicht jedoch auch ein großflächiger oder kompletter Ausfall von Satelliteninfrastruktur in Planungen berücksichtigt werden. Dieses Szenario kann nicht nur durch einen Angriff hervorgerufen werden. Durch starke Sonneneruptionen ausgelöste geomagnetische Stürme können in einem Carrington-Ereignis Infrastruktur auf der Erde und insbesondere im Orbit zerstören, bei nur wenigen Stunden Vorwarnzeit. Bei dem namensgebenden Vorfall 1859 traten weltweit Störungen und spontane Entzündungen in Telegraphen-Stationen auf, die Auswirkung auf unsere heutige Gesellschaft wären ungleich größer. Wenngleich Eisbohrkerne ein Auftreten solcher geomagnetischer Stürme ca. alle 500 Jahre zeigen, entging die Erde 2012 nur knapp einem solchen Ereignis.

Umfangreiche Zerstörungen von Satelliten im LEO ließen sich auch mit Hilfe eines elektromagnetischen Impulses (EMP) durch Nukleardetonationen hervorrufen, der in Sichtlinie direkt ungeschützte Satelliten treffen und durch die verbleibende Strahlung auch nachfolgende Satelliten beschädigen würde. Da ein EMP jedoch alle Infrastruktur beschädigen würde und sich nicht ohne eigene und große, langanhaltende Kollateralschäden einsetzen ließe, ist diese Option unattraktiv für Nationen mit Interessen im Weltraum.

Zerstörung von Orbits

Signifikanter Nachteil von kinetischen Mitteln ist die große Menge an Trümmern, die im LEO ein Jahrzehnt – in höheren Orbits auch Jahrhunderte – verbleiben und andere Satelliten beschädigen bzw. sogar ebenfalls zertrümmern können. So ließ der chinesische Abschuss eines ausrangierten Wettersatelliten 2007 mehr als 3.000 große und verfolgbare Bruchstücke, sowie weit mehr als 100.000 kleine Teile in der Umlaufbahn zurück. Ebenso entstanden Tausende Trümmerteile zwei Jahre später durch die Kollision des US-Satelliten Iridium-33 mit dem defekten russischen Satelliten Cosmos 2251. Das US-amerikanische Space Surveillance Network katalogisiert und verfolgt aktuell die Flugbahn von etwa 20.000 Objekten, weitere geschätzte 500.000 Objekte kleiner als 10 cm entgehen jedoch einer Überwachung.

Mit der stark zunehmenden Nutzung der Orbits sowie der mittlerweile drastischen Verunreinigung steigt das Risiko für ein Kessler-Syndrom, bei dem die Trümmer eines Satelliten wiederum andere Satelliten zerstören, und in einer Kettenreaktion die . Dieses Szenario wurde im Hollywood-Film „Gravity“ 2013 dargestellt; wenngleich das Problem seit den 70er Jahren bekannt ist, steigt in den letzten Jahren durch neue LEO-Konstellationen die Anzahl der Objekte so sehr an, dass wahrscheinlich ein Wendepunkt erreicht wird [11], sodass kostspielige Maßnahmen nötig werden und Weltraum-Nutzung in populären Orbits nur noch nach anderen als den aktuell etablierten Parametern möglich sein könnte. Schon heute bekommt ein LEO-Satellit Hunderte von Annäherungs-Alarmen pro Woche [4], mit dem weiteren Ausbau und Markteintritt von neuen Mega-Konstellationsbetreibern wird das weiter steigen. Auch wenn ein Kessler-Syndrom „nur“ in einem niedrigen Orbit auftreten sollte, könnte es dennoch erhebliche Auswirkungen auf die Möglichkeit haben, Satelliten in höheren Umlaufbahnen platzieren zu können, da Trägerraketen den Trümmerring nicht mehr ohne Kollision durchfliegen können. Bereits heute müssen Startzeitfenster für Starts in Abhängigkeiten von Flugbahnen katalogisierter Trümmerteile gewählt werden.

Alternative Möglichkeiten

Ergebnis der oben skizzierten Szenarien ist der temporäre oder permanente Verlust kritischer Satelliteninfrastruktur. Abgesehen von den damit verbundenen Kosten und Wiederherstellungszeiten könnte im schlimmsten Fall hiermit eine dauerhafte Einschränkung der Ressource Weltraum einhergehen, so dass z. B. erst nach Jahrzehnten die Trümmerdichte durch natürlichen Wiedereintritt so weit abgenommen haben könnte, dass neue Systeme ausgebracht werden können. Technische Möglichkeiten zum Einfangen und zur Beseitigung von Trümmern in der Umlaufbahn sind Gegenstand aktiver Forschung. Auch wenn technische Herausforderungen in den kommenden Jahren überwunden werden, bedeuten der große Energiebedarf und damit verbundene finanzielle Aufwand, aber auch fehlende Anreize, dass hier zeitnah mit keiner Abhilfe zu rechnen ist.

Der Ausfall der technischen Nutzbarkeit der Ressource Weltraum hätte weitreichende Konsequenzen. So bietet GPS nicht

nur Positionsbestimmung für Logistik, See- und Luftfahrt, sondern dient auch der Synchronisation der Zeit in Energienetzen und anderer kritischer Infrastruktur. Globale Kommunikation, Fernsehübertragungen, Wetter- und Erdbeobachtung wären eingeschränkt.

Eine mögliche Nichtverfügbarkeit von Satelliten im Konfliktfall würde auch Annahmen über die Durchführung und Rahmenbedingungen von Militäroperationen verändern, und sollten bereits jetzt in einer Kontingenzplanung vorgedacht und ausstaffiert werden. So könnten Fähigkeiten in der Aufklärung und Kommunikation zum Teil, aber eben nicht vollständig durch luftbasierte Systeme substituiert werden, und Alternativen für die Deckungslücke erarbeitet werden. Die Vernetzung von Truppen könnte z. B. mit Hilfe von Stratosphären-Ballons ermöglicht werden, die zum einen kostengünstig, zum anderen auch schnell replizierbar ausgebracht werden können. Googles Project Loon konnte demonstrieren, dass diese Plattformen langlebig und positionsstabil genug sind [2], um für einen solchen Zweck eingesetzt werden zu können.

Bislang gibt es nur vereinzelte Skizzen über mögliche Alternativen und Rückfalloptionen zur Ressource Weltraum. Vorreiter sind die Vereinigten Staaten mit der Etablierung des US Operationally Responsive State Office, welches ein 3-stufiges Notprogramm zur schnellen Reaktion auf den Verlust von militärischen Weltraum-Infrastrukturen entwickelt [13]. So können im ersten Reaktionsschritt innerhalb von Stunden bis Tagen existierende Boden- und Weltraumplattformen umgewidmet werden. Sollte keine nutzbare Infrastruktur mehr verfügbar sein, können im zweiten Schritt im Rahmen von 24 Stunden lagernde Satelliten mit bereitstehenden Raketen ausgebracht werden [18]. Fehlende Fähigkeitslücken werden dann im dritten Schritt nachentwickelt, produziert und sollen im Rahmen von wenigen Monaten bis Jahresfrist im Einsatz sein. Doch nicht nur neue Satelliten könnten im Verteidigungsfall nötig sein, auch die kurzfristige, gezielte Entfernung gegnerischer Satelliten aus der Umlaufbahn wäre von großem Interesse: so hat China die prinzipielle Möglichkeit bewiesen auch im GEO per Satellit andere Objekte zu manipulieren und entfernen, auch die autonom agierende U.S.-amerikanische X-37B mit einer Ladebuch und der Fähigkeit mehrjährige Missionen im Orbit durchzuführen, sollte in diesem Kontext betrachtet werden.

Je nach Schadensszenario – z. B. einem unfallbedingten oder vorsätzlich herbeigeführten Kessler-Syndrom – ist ein Neustart von Satelliten in vergleichbare Orbits für längere Zeit jedoch keine Option, und Trümmfelder können auch den Zugang zu höher gelegenen Orbits erschweren. In diesen Fällen braucht es einen Plan B – auf der Erde.

References

- [1] Lin, H, Qing, Y., GPS spoofing – low-cost GPS simulator, DEFCON 2023, <https://en.calameo.com/read/004474480397d2632c1e3>
- [2] Rieger, F., "Wettrüsten mit Ballons in der Stratosphäre," 2023, <https://steadyhq.com/de/realitatsabzweig/posts/90669d9fe2f2-4793-a213-be6570e77d80>
- [3] Bloembergen, N., C. K. N. Patel, P. Avizonis, R. G. Clem, A. Hertzberg, T. H. Johnson, T. Marshall, R.B. Miller, W. E. Morrow, E. E. Salpeter, A. M. Sessler, J. D. Sullivan, J. C. Wyant, A. Yariv, R. N. Zare, A. J.Glass, L. C. Hebel, G. E. Pake, M. M. May, W. K. Panofsky, A. L. Schawlow, C. H. Townes, und H. York, "Report to the American Physical Society of the study group on science and technology of directed energy weapons," *Reviews of Modern Physics* 59 (3), 1987.
- [4] Buchs, R., "Collision risk from space debris: Current status, challenges and response strategies." International Risk Governance Center, 2021
- [5] Futron Corporation, "U.S. government market opportunity for commercial satellite operators: For today or here to stay," 2003
- [6] Elgin, B., "Network security breaches plague NASA," Bloomberg, 19. November 2008, <https://www.bloomberg.com/news/articles/2008-11-19/network-security-breaches-plague-nasa>
- [7] Secure World Foundation, "Global counterspace capabilities – An Open Source Assessment," 2022
- [8] Ganguli, G., C. Crabtree, L. Rudakov, und S. Chappie., "A concept for elimination of small orbital debris," *Transactions of the Japan Society for Aeronautical and Space Sciences* 10 (ists28), 2012

- [9] Geovedi, J., R. Iryandi und A. Zboralski, "Hacking a bird in the sky: Exploiting satellite trust relationship," Hack in theBox Security Conference, 2008
- [10] Honrada, G., "China claims laser weapon gain on US space dominance," Asia Times, 14. August 2023
- [11] McKnight, D. und D. Kessler, "We've already passed the tipping point for orbital debris," IEEE Spectrum, 2012
- [12] Mount, M. und E. Quijano, "Iraqi insurgents hacked predator drone feeds, U.S. official indicates," CNN, 18. Dezember 2009, <https://edition.cnn.com/2009/US/12/17/drone.video.hacked/index.html>
- [13] U.S. Department of Defense, "Plan for operationally responsive space – a report to congressional defense committees," U.S. Department of Defense – National Security Space Office, 2007
- [14] U.S. Department of Defense, "Military and security developments involving the Peoples Republic of China," Annual Report to Congress, U.S. Department of Defense, 2020
- [15] Office of Director of National Intelligence, "Support to U.S. space command messaging," 2020
- [16] Pavur, J., D. Moser, M. Strohmeier, V. Lenders und I. Martinovic, "A tale of sea and sky on the security of maritime VSAT communications," IEEE Symposium on Security and Privacy, 2020
- [17] Wilson, C., "Network centric warfare: Background and oversight issues for congress," Library of Congress Congressional Research Service, 2004.
- [18] Bridenstine, J., "Tactically Responsive Space strengthens America", SpaceNews, 18. September 2023

Quellenangaben

Titelbild von somneuk (Generiert mit KI – Telecommunication satellite providing global internet network and high speed data communication above Europe) – stock.adobe.com