Schulze, Matthias

Research Report

Cyber-Sicherheit im Weltraum: Verwundbarkeiten, Angriffsvektoren und Schutzmaßnahmen

SWP-Aktuell, No. 4/2023

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Schulze, Matthias (2023) : Cyber-Sicherheit im Weltraum: Verwundbarkeiten, Angriffsvektoren und Schutzmaßnahmen, SWP-Aktuell, No. 4/2023, Stiftung Wissenschaft und Politik (SWP), Berlin, https://doi.org/10.18449/2023A04

This Version is available at:
https://hdl.handle.net/10419/268790

SWP

SWP-Aktuell

NR. 4 JANUAR 2023

Cyber-Sicherheit im Weltraum

Verwundbarkeiten, Angriffsvektoren und Schutzmaßnahmen

Matthias Schulze

Die IT-Sicherheit von Weltrauminfrastrukturen wird relevanter, während sich zahlreiche Staaten einen neuen Wettlauf um das All liefern. Cyber-Operationen gegen entsprechende Ziele nehmen zu; so wurde etwa im Zuge des russischen Einmarschs in die Ukraine ein Kommunikationssatelliten-Netzwerk von Hackern angegriffen. Regierungen sollten daher Mindeststandards für die IT-Sicherheit im Weltraum definieren; ebenso gilt es, frühzeitig einen Informationsaustausch zwischen Staaten und privaten Akteuren zu initiieren, was Cyber-Bedrohungen und »best practices« zur Härtung der Infrastrukturen betrifft. Innerhalb von EU und Nato könnten wechselseitig Daten über Bedrohungslagen weitergegeben werden; ebenso ist die Schaffung von Computer Emergency Response Teams zu erwägen. Auch mit »Hacking-Wettbewerben« und gemeinsamen Übungen ließe sich dazu beitragen, die IT-Sicherheit im All zu verbessern.

Der russische Angriffskrieg gegen die Ukraine belegt, wie relevant das Thema IT-Sicherheit von Weltrauminfrastrukturen ist. Es geht hier um Satelliten, Raumstationen, unbemannte Flugsysteme (Sonden) sowie Weltraum-Boden-Kontrolleinrichtungen wie etwa Terminals. Am 24. Februar 2022, dem Tag der russischen Invasion, störte eine Cyber-Operation das KA-SAT-Kommunikationssatelliten-Netzwerk über Südosteuropa. Die ukrainische Militärkommunikation sollte behindert werden, um Russlands Streitkräften das Vorrücken zu erleichtern. Allerdings wurde nicht nur militärische Internetkommunikation über Satelliten gestört, sondern als Kollateralschaden auch die Steuerungsinfrastruktur tausender Windenergieturbinen in Europa, darunter in Deutschland. Wie sich später herausstellte, wurden die Satellitenmodems mittels einer Wiper-Schadsoftware (AcidRain) gelöscht, die Russland attribuiert wurde. Der Vorfall zeigte, wie verwundbar Weltrauminfrastrukturen gegenüber Cyber-Operationen prinzipiell sind.

Zudem entwickeln immer mehr Bedrohungsakteure sogenannte »soft kill counterspace«-Fähigkeiten. Dabei geht es um Maßnahmen, mit denen Satelliten lahmgelegt werden, etwa mittels elektronischer Kampfführung. Zu dieser gehören das »jamming«, also das Stören des Empfangs, und das »spoofing« — das Fälschen von Signalen —, der Einsatz von Mikrowellenwaffen, Blendung durch Laser und überdies Cyber-Operationen. Soft-kill-Fähigkeiten sind eine Alternative zu Antisatellitenwaffen (ASAT). Letztere sollen Satelliten kinetisch zerstö-

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

ren, etwa durch Raketenbeschuss oder Sabotage im Orbit. China, Indien, Russland und die USA haben bereits konventionelle ASAT-Waffen vorgeführt. Werden Satelliten physisch zerstört, besteht allerdings das Risiko einer unkontrollierten kaskadenförmigen Freisetzung von Weltraumschrott (alias Kessler-Syndrom). Ein Weg, diese Gefahr zu umgehen, ist Hacking, das auch geringere Kosten mit sich bringt und dessen Effekte reversibel sind. Cyber-Operationen sind zudem eine Grauzonen-Aktivität, deren Entdeckung unwahrscheinlicher ist und die folglich eher weniger gravierende Konsequenzen für Angreifer hat. Darüber hinaus können Staaten ohne eigenes Weltraumprogramm, wie der Iran oder Nordkorea, ihre Cyber-Einheiten ohne größere Kosten auf Weltrauminfrastruktur ausrichten. Damit lassen sich für sie asymmetrische Vorteile generieren, denn Satellitenkommunikation ist eine Achillesferse des US-Militärs.

Da Cyber-Operatoren von ihren Konkurrenten lernen und auf die Nutzung asymmetrischer Vorteile bedacht sind, ist es für Bedrohungsakteure lukrativ, Satelliten mittels Cyber-Operationen ins Visier zu nehmen. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) betont, dass Weltrauminfrastruktur einen »Single Point of Failure« darstellt, bei dem mit überschaubarem Aufwand enormer Schaden angerichtet werden kann. Zu den gängigen Motiven für Staaten, entsprechende Aktivitäten zu starten, gehören wohl Spionage (durch Diebstahl geistigen Eigentums oder Abfangen der Datentransmissionen etwa von Spionagesatelliten), Manipulation von Kommunikation sowie das Verursachen temporärer Störungen bis hin zur Unbrauchbarmachung von Satelliten, um taktische Vorteile zu erlangen, etwa im Kontext eines bewaffneten Konflikts. Weltraumunternehmen mit größeren Gewinnen könnten auch für erpresserische Ransomware-Angriffe von Cyber-Kriminellen interessant sein.

Der Weltraum: Relevanz und aktuelle Trends

Seit einigen Jahren lässt sich eine intensivierte Militarisierung des Weltraums verfolgen, wie sie auch im Cyber- und Informationsraum (CIR) stattfindet. Verteidigungsetats wachsen, und die Modernisierung von Weltraumsystemen schreitet voran. 2019 gründeten die USA ihre militärische Space Force und definierten den Weltraum als Domäne der Kriegführung, wie es auch die Nato tat. Im selben Jahr wurde ein vermutlich iranischer Bedrohungsakteur dabei beobachtet, wie er US-Satellitenunternehmen mittels Cyber-Operationen angriff. Bereits 2018 infizierten mutmaßlich chinesische Hacker amerikanische Bodenstationen zur Kontrolle von Satelliten. Das Ziel war anscheinend, Know-how zum Betrieb eigener Weltrauminfrastruktur in China zu stehlen. Theoretisch wäre es den Angreifern auch möglich gewesen, die orbitale Position von Satelliten zu verändern und so etwa Kollisionen zu verursachen. Nichtstaatliche Akteure zeigen ebenfalls Interesse daran, Weltrauminfrastruktur zu hacken. Im Kontext des Ukraine-Krieges 2022 hat das Kollektiv »Anonymous« nach eigenen Angaben russische Weltraumforschungszentren und die Agentur Roscosmos gehackt. Dabei wurden Daten des Mondprojekts Luna Resource Mission gestohlen und veröffentlicht.

Die Relevanz von Weltrauminfrastrukturen hat mit dem »New Space Race« der letzten Jahre zugenommen. Um 2010 gab es jährlich noch rund 130 Starts ins All, mittlerweile sind es knapp 2 000. Rund 72 Länder haben heute ein Weltraumprogramm, darunter Brasilien, Indien, China und die Vereinigten Arabischen Emirate. Hinzu kommt eine Machtverschiebung hin zu privaten Akteuren — das All ist nicht mehr nur eine Domäne von Staaten. Viele Weltrauminfrastrukturen sind »dual use«, haben also eine kommerzielle und eine militärische Komponente, so etwa das Global Positioning System (GPS). Unternehmen wie SpaceX und Blue Origin suchen die Kosten für Weltraumtransporte durch wiederverwertbare Raketen massiv zu reduzieren.

Auch die Produktionspreise von Satelliten sinken, denn verwendet werden zunehmend »Commercial Off-the-Shelf« (COTS)-Hardware, Open-Source-Software und neue Dienstleistungen wie »Ground Station as a Service«. Dies macht wiederum neue Anwendungen wie satellitengestützte Internetkommunikation, darunter Elon Musks Starlink, rentabler und relevanter. Unter anderem greift die Ukraine im aktuellen Krieg auf Starlink-Systeme zurück, um an der Front Redundanz für terrestrische Internet-Datenverbindungen zu schaffen, die durch Beschuss und Cyber-Operationen immer wieder ausfallen.

Neben Starlink tummeln sich mehr und mehr Start-ups auf dem Markt, deren IT-Sicherheit nicht immer optimal aufgestellt ist. Es gibt einen anhaltenden Trend zu Megakonstellationen sogenannter Low Earth Orbit (LEO)-Satelliten, die sich auf einer niedrigen Erdumlaufbahn bewegen. Sie werden in naher Zukunft essentiell sein für das Internet der Dinge (IoT), für autonome Systeme und für die Internetkonnektivität in ländlichen Gegenden des globalen Südens (vgl. SWP-Studie 2/2021). Schon bald dürften Satelliten eine eigene Art Internet-Backbone bilden, das für die Kommunikation zahlreicher kritischer Infrastrukturen und auch für interplanetare Kommunikation relevant ist. Weltraumbasierte Dienste sind heute schon maßgeblich für das Militär, vor allem in Nato-Staaten (bei Leitsystemen für Waffen, Command and Control), für Verkehr und Logistik (z.B. durch GPS in der Seenavigation), Landwirtschaft (»precision farming« und Überwachung von Feldern), Finanzdienstleistungen sowie Notfall- und Katastrophenschutz. Immer mehr IoT-Geräte und Smartphones werden ebenfalls diese Technologie nutzen, insbesondere dort, wo 5G-Mobilfunknetze keine gute Netzabdeckung erlauben.

Ein Verlust oder ein Ausfall von Weltrauminfrastruktur als Folge einer Cyber-Operation könnte sich — je nach Umfang und Intention des Angriffs — auch für die Bundesrepublik fatal auswirken. Der Weltraum muss deshalb als eine emergente kritische Infrastruktur behandelt werden, die nicht unter der Souveränität eines einzelnen Staates steht, von der aber, wie auch vom Internet, zahlreiche kritische Prozesse abhängen. Für Deutschland gilt zudem, dass man hochgradig von Ländern wie Russland und den USA abhängig ist, will man Infrastruktur ins All befördern.

Die IT-Sicherheitsdimension von Weltrauminfrastrukturen

Weltrauminfrastruktur wird nicht nur billiger, sie wird auch immer komplexer. Komplexität ist allerdings der logische Gegensatz von IT-Sicherheit. Während frühe Satelliten einfache Signalverstärker mit begrenztem Funktionsumfang waren, sind heutige Systeme immer stärker software-gestützt. Sie sind miteinander vernetzt, um im Verbund Funktionen auszuführen. Und sie können im All rekonfiguriert werden, etwa um sich dynamisch neuen Bedarfen anzupassen.

Mehr Software bedeutet aber, dass die IT in Weltrauminfrastrukturen immer mehr den gleichen Problemen ausgesetzt ist wie terrestrische Systeme. Forscher fanden etwa 2018 heraus, dass die Betriebssysteme vieler kommerzieller Satellitenterminals, die im Schiffs- und Luftverkehr genutzt werden, mit unzureichenden IT-Sicherheitsmaßnahmen versehen waren. Dabei zeigten sich klassische Probleme wie fest codierte Zugangsdaten, unsichere und nicht dokumentierte Kommunikationsprotokolle sowie eine generell schlechte Programmierung mit zahlreichen Sicherheitslücken. Bisweilen wurden keine oder veraltete Verschlüsselungsalgorithmen bzw. Protokolle für die Bodenkommunikation genutzt. COTS-Hardware und -Software kann aufgrund komplexer Lieferketten Hintertüren beinhalten. Satelliten bestehen aus tausenden Bauteilen, die weltweit produziert werden. Insofern ist das Risiko nicht auszuschließen, dass bei vielen Satelliten eine nachrichtendienstliche Mitnutzung erfolgt. Weltraumsysteme benötigen zudem Fernzugriffskanäle, die kompromittiert werden können. Sie brauchen regelmäßig Software-

Updates und Wartungsdowntimes, um Sicherheitslücken zu schließen.

Der Einsatz im Weltraum erfordert zudem eigene IT-Sicherheitspraktiken, die von denen terrestrischer IT-Systeme abweichen. Satelliten werden im Durchschnitt 15 Jahre lang verwendet. Teilweise sind noch ältere Modellgenerationen der frühen 2000er Jahre im Einsatz, die nicht von vornherein mit »security by design« entwickelt wurden. Solche »Legacy-Systeme« verwenden meist ältere Software, die nicht einfach gepatcht werden kann. Oftmals ist es also nicht möglich, die IT-Sicherheit im operativen Betrieb im All nachträglich anzupassen. Stattdessen müssen Satelliten zukunftsfähig sein, das heißt, wahrscheinliche Angriffsszenarien der nächsten 10 bis 15 Jahre sind schon bei der Entwicklung zu antizipieren. Ein besonderes Problem sind dabei hardware-seitige, in Bauteilen angelegte Schwachstellen, die nicht per Software-Update behoben werden können, also über die gesamte Lebensdauer eines Satelliten eine Angriffsfläche darstellen. Hacker demonstrieren immer wieder, dass man die Kommunikation veralteter Systeme mit geringen Investitionskosten »spoofen«, also durch manipulierte Signale in die Irre führen kann.

Aber auch moderne Systeme lassen sich ohne größeren Aufwand hacken. Auf der »Black Hat«-Sicherheitskonferenz in Las Vegas wurde im August 2022 gezeigt, dass man mit Ausrüstung für 25 US-Dollar zur Modifikation von Hardware (Modding) einen manipulierten Software-Code auf Starlink-Terminals ausführen kann. Der Angriff basiert auf einer Hardware-Schwachstelle, die bei den rund 3 000 vorhandenen LEO-Starlink-Satelliten im Weltall nicht einfach beseitigt werden kann. Starlink reagierte bereits mit einer Fehlerbehebung, so dass von dem Angriffsvektor, der zudem physischen Zugriff auf Terminals erfordert, kein größeres Risiko mehr ausgehen dürfte (LEO-Satelliten haben eine geringe Lebenszeit). Allerdings zeigt das Beispiel eine generelle Verwundbarkeit, die durch eine größere Anzahl von Satelliten und Marktteilnehmern, die in der IT-Sicherheit nicht alle überzeugende »best practices« vorweisen können, eher zunehmen. Geld ist dabei ein Faktor. Ein Mehr an IT-Sicherheitsfeatures treibt Entwicklungskosten in die Höhe, weshalb hier teils Abstriche gemacht werden.

Angriffsfläche und Vektoren

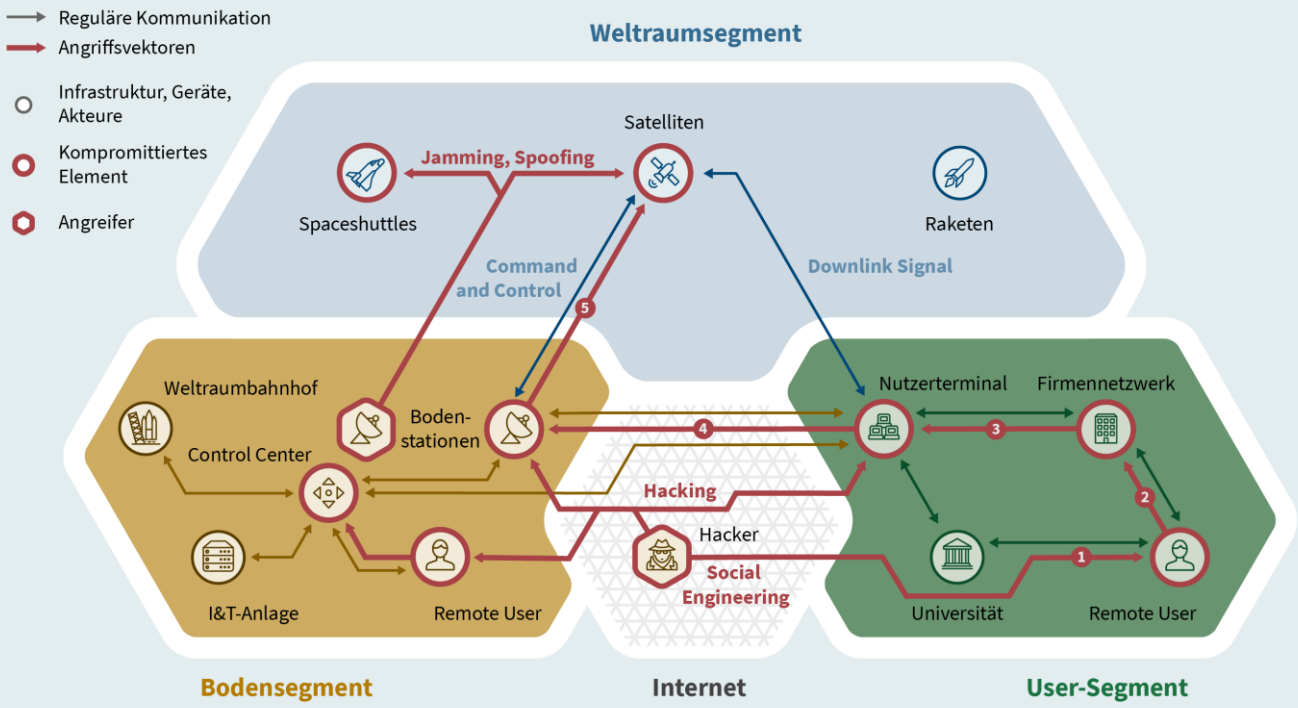
Weltrauminfrastruktur bietet eine große Angriffsfläche für bösartige Akteure. In der Regel unterscheidet man dabei zwischen dem Weltraumsegment, dem Bodensegment und dem User-Segment (siehe Grafik). Das Weltraumsegment umfasst Satelliten und Weltraumfahrzeuge. Das Bodensegment unterteilt sich in Bodenstationen, die etwa über Antennen eine direkte Kommunikation mit dem Weltraumsegment gewährleisten, Mission Control Center, welche Raumfahrzeuge steuern und verwalten, sowie verschiedene, mitunter auch mobile Zugangsterminals (z.B. für militärische Auslandseinsätze). All diese Elemente sind durch verschiedene Bodennetzwerke miteinander verbunden. Oft sind die entsprechenden Einrichtungen über den Globus verteilt, um dauerhafte Sichtverbindungen zum Satelliten zu garantieren und um eine Ausfallredundanz sicherzustellen. Solche Netzwerke erlauben zudem oft internetbasierte Remote-Verbindungen für wissenschaftliches und technisches Personal.

Deshalb sind die Netzwerke vielfach für internetbasierte Angriffsvektoren verwundbar. Social Engineering wie Spear-Phishing, also das Ködern von Personal mit privilegiertem Zugang durch manipulierte E-Mails, kann hier ansetzen. Wie überall ist die Gefahr von Insider-Bedrohungen nicht zu unterschätzen. Aufgrund dieser Vulnerabilität ist das Bodensegment in der Regel der primäre Zugriffspunkt für Cyber-Operationen gegen Weltrauminfrastruktur.

Das User-Segment umfasst die Bereitstellung von Dienstleistungen an Dritte, etwa über Schnittstellen zur Abfrage von Orbitaldaten oder durch kommerzielle Vermietung von Erdbeobachtungssatelliten. Sind die Segmente nicht gut voneinander isoliert, ist etwa das Corporate-Netzwerk eines Unternehmens nicht logisch und physisch vom Bodensegment getrennt, bieten sich

Grafik

Segmente von Weltraum-Infrastruktur



Diese Grafik ist in der Farbdarstellung am besten lesbar.

Quelle: https://en.wikipedia.org/wiki/Ground_segment#/media/File:Ground_segment.png

hier Einfallstore für Cyber-Operationen. Gelingt Angreifern der Zugriff auf eine Bodenstation, lassen sich darüber dann theoretisch auch Satelliten erreichen. Direkte Cyber-Operationen gegen Satelliten sind eher untypisch, weil es dazu eigener Antennen und Bodeninfrastruktur bedarf. Hier kommen also eher staatliche Akteure in Frage, auch wenn sich das durch die Machtverschiebung hin zum Privatsektor ändert. Mit den genannten Mitteln wären allerdings »spoofing«-Angriffe gegen fremde Satelliten denkbar, also die Eingabe falscher Steuerungsbefehle, etwa durch die Manipulation älterer, unsicherer Kommunikationsprotokolle. Auch ist es in naher Zukunft denkbar, dass Mobilfunkstationen oder IoT etwa auf dem Mond oder einer hypothetischen Marskolonie ebenfalls ein Angriffsvektor sein können.

Maßnahmen zur Verbesserung von IT-Sicherheit im Weltraum

Der Start von US Space Command im Jahr 2019 markierte einen Meilenstein in den Bemühungen des amerikanischen Militärs, die Sicherheit von Weltrauminfrastrukturen zu verbessern. Space Command versteht Cyber-Operationen dezidiert als eine Anwendung von »space power«, die man auch gegenüber Gegnern nutzen will. 2019 startete ebenfalls das Space Information Sharing and Analysis Center (Space ISAC), das den Austausch von Bedrohungsdaten über verschiedene US-Behörden und Privatunternehmen hinweg ermöglichen soll. Dazu gehören explizit auch Informationen zu Cyber-Bedrohungen, die über ein eigenes Datenportal geteilt werden. Später sollen ebenso klassifizierte Daten geteilt werden.

Im Mai 2021 verkündete die amerikanische Cybersecurity and Infrastructure Security Agency (CISA) den Aufbau einer Space Systems Critical Infrastructure Working Group. Es handelt sich dabei um eine Public-Private Partnership, die Stakeholder aus dem Bereich kritischer Weltrauminfrastrukturen zusammenbringt. Die Arbeitsgruppe soll Lösungen und »best practices« zur Verbesserung der IT-Sicherheit von »space assets« identifizieren und entwickeln.

Gegenwärtig wird in den USA mit dem Space Infrastructure Act zudem ein Gesetzentwurf diskutiert, der Weltrauminfrastruktur zum 17. Sektor der kritischen Infrastruktur (KRITIS) erheben soll. Damit würde die amerikanische Regierung größere Befugnisse zur Mandatierung von IT-Sicherheit erhalten. Raumfahrtunternehmen und das Space ISAC unterstützen das Vorhaben, während die Biden-Regierung laut National Cyber Director Chris Inglis gegenwärtig kein Interesse daran hat. Der Weltraum transzendiere gewissermaßen die Sektorengrenzen und passe nicht in das Gefüge der anderen 16 kritischen Infrastrukturen, so Inglis. Er halte es daher nicht für sinnvoll, das All gesondert verteidigen zu wollen. Stattdessen möchte Washington nun kritische Funktionen identifizieren, welche die Grenzen der bestehenden KRITIS-Sektoren überschreiten, um diese separat zu schützen. Der Weltraum spielt dabei eine besondere Rolle. Ähnliche Diskussionen gibt es in anderen Ländern. Großbritannien und Frankreich haben Weltrauminfrastruktur bereits als KRITIS designiert.

In der EU erschien Anfang 2023 die aktualisierte Fassung der Richtlinie für Network and Information Systems (NIS 2), die ebenfalls um Weltrauminfrastrukturen erweitert wurde. Die Direktive beinhaltet viele sinnvolle IT-Sicherheitsanforderungen — darunter Risikoanalyse, Incident Handling, Audits sowie die Pflicht für Betreiber, Kommunikation zu verschlüsseln. Allerdings hat NIS 2 auch erkennbare Schwächen. Sie greift in erster Linie für EU-eigene Weltrauminfrastrukturen (etwa Galileo) bzw. nur für jene Sektoren, die von Mitgliedstaaten als kritische Infrastruktur definiert wurden. Das heißt, die Staaten müssen eigene Weltrauminfrastrukturen zunächst per nationalem Gesetz entsprechend kategorisieren, bevor die Direktive in Zukunft wirken kann. Zudem betrifft die Richtlinie bisher nur das Bodensegment. Für das ebenso verwundbare Weltraumsegment fehlen verpflichtende IT-Sicherheitsanforderungen. NIS 2 deckt zudem nicht zwingend Satelliten von Mitgliedstaaten ab. Diese müssen die Richtlinie zunächst implementieren und haben natürlich Spielräume bei der Umsetzung in nationales Recht. Die Direktive hat also blinde Flecken. Der Vorteil von NIS 2 ist jedoch, dass das aktuelle Momentum genutzt werden könnte, um internationale technische Standards (etwa ISO) für die IT-Sicherheit von Weltrauminfrastrukturen zu definieren.

Entwicklungen in Deutschland

In Deutschland haben seit der Verabschiedung der Raumfahrtstrategie von 2010 diverse Prozesse begonnen, um die (IT-)Sicherheit von Weltrauminfrastrukturen zu verbessern. Seit 2009 gibt es bei der Bundeswehr das Lagezentrum Weltraum, welches ein Lagebild der im All befindlichen Objekte erstellen soll (dabei aber auf die Hilfe internationaler Partner angewiesen ist). 2017 veröffentlichte das Verteidigungsministerium die Strategische Leitlinie Weltraum. Potentielle Bedrohungen sollen damit erfasst und geeignete Schutzmaßnahmen etabliert werden. Zu diesem Zweck entstanden diverse ressortübergreifende Arbeitsgruppen und Konferenzen. Die Cyber-Sicherheitsstrategie des Bundesinnenministeriums von 2021 versteht weltraumbasierte Infrastruktur, zusammen mit 5G-Infrastruktur, als »Rückgrat der Digitalisierung der Gesellschaft«, welche »fortlaufend evaluiert und an neue Gefährdungen angepasst« werden soll.

Allerdings scheint noch nicht abschließend geklärt, wer für die IT-Sicherheit von Weltrauminfrastrukturen jenseits des Bodensegments zuständig ist. Das deutsche BSI veröffentlichte jüngst ein Positionspapier zum Thema. Demnach versteht man

die Bodeninfrastruktur von Satellitensystemen ebenfalls als kritische Infrastruktur, die in den Kompetenzbereich des BSI gehöre. Damit greift auch die KRITIS-Verordnung. Ob sie für im All befindliche Systeme ebenso gilt, scheint bislang jedoch offen. Dies sollte in Zukunft durch ein nationales Weltraumgesetz definiert werden, da freiwillige Selbstverpflichtungen aus der Industrie in der Regel nicht reichen, um die IT-Sicherheit zu erhöhen.

Das BSI hat bereits ein Schwerpunktreferat für Informationssicherheit im All eingerichtet. In den kommenden Jahren will das Amt Mindestanforderungen für die Weltraum-Cybersicherheit identifizieren und dazu technische Richtlinien veröffentlichen. Dies ist insofern sinnvoll, als dass damit eine wichtige Orientierungshilfe für deutsche Weltraumunternehmen geschaffen wird. Allerdings handelt es sich eben um bloße Richtlinien und nicht um Pflichten.

Zu den technischen Mindestanforderungen, die neue Weltrauminfrastrukturen erfüllen sollten, gehören unter anderem: »security by design« für die Software-Entwicklung; Standard-Cyber-Hygienemaßnahmen wie das Verbot von »hard coded«-Zugangsdaten, umfassendes Logging und Anomaliedetektion; Netzwerksegregation sowie Identitäts- und Zugangsmanagement für alle Segmente; Risikomanagement für Versorgungsketten (»supply chain«). Alle bodengestützten Systeme sollten zwingend Incident Response (zur Reaktion auf Vorfälle), Business Continuity (für einen unterbrechungsfreien Betrieb) und Verfahren zur Krisenkommunikation entwickeln. Das gilt gleichermaßen für zivile Satellitenbetreiber wie z.B. Universitäten; auch sie müssen zum Schutz kritischer Infrastruktur beitragen, die für die nationale Sicherheit relevant ist.

Das neugeschaffene Weltraumkommando der Bundeswehr, das seit 2021 einsatzfähig ist, kann bei der IT-Sicherheit ebenfalls eine Rolle spielen. Dort arbeiten die Inspekteure der Luftwaffe und des Kommandos Cyber- und Informationsraum (KdoCIR) mit zivilen Experten des Deutschen Zentrums für Luft- und Raumfahrt zusammen. Die Bundeswehr beansprucht für sich, im Weltraum operationsfähig zu werden, und zwar ausschließlich defensiv. Offensive ASAT-Fähigkeiten konventioneller Art sind nicht vorgesehen. Ob dies auch für Cyber-Fähigkeiten gilt, ist unklar. Im Vordergrund stehen der Schutz der eigenen Weltraumsysteme, das Sammeln von Informationen zur Lage im All und die Sicherstellung von Kommunikation und Aufklärung bei Auslandseinsätzen. Auch arbeitet das Verteidigungsministerium gegenwärtig an einer Weltraumverteidigungsstrategie, welche diese Punkte konkretisieren soll.

Die Beteiligung des KdoCIR an der IT-Sicherheit im Weltraum ist insofern sinnvoll, als das Kommando einen internationalen Anknüpfungspunkt für Alliierte bilden kann, um »best practices« zur IT-Sicherheit auszutauschen. Das KdoCIR könnte zudem seine Red-Teaming-Fähigkeiten einsetzen, also eigene Hacker auf eigene Weltrauminfrastruktur loslassen, um potentielle Schwachstellen und Einfallsvektoren zu identifizieren und zu beheben. Eine andere Idee wären Hacking-Wettbewerbe. Die US-Luftwaffe organisiert mittlerweile regelmäßig das »Hack a Sat«-Turnier, dessen Teilnehmer in Testumgebungen Satelliten angreifen und die gefundenen Schwachpunkte dem Militär melden. Die Abwehr von Cyber-Angriffen gegen Satelliten sollte zudem vermehrt auf entsprechenden Trainingsanlagen (Cyber Ranges), bei multinationalen Übungen wie »Locked Shields« und in »wargaming«-Simulationen erprobt werden. Auch dazu können die Cyber-Einheiten des KdoCIR beitragen.

Multilaterale Maßnahmen

Nationale Anstrengungen sind sinnvoll, aber vermutlich nicht ausreichend. Die internationale Governance des Weltraums wiederum hält mit der aktuellen Dynamik nicht Schritt. Der Weltraumvertrag von 1967 garantiert sämtlichen Staaten freien Zugang zum All, postuliert dessen gemeinwohlorientierte Erforschung und verbietet die Aneignung fremder Weltraumobjekte. Zwar sind Nuklearwaffen im Weltraum verboten, nicht aber zwingend »soft kill

counterspace«-Fähigkeiten. Andere Vertragswerke wie die Space Liability Convention von 1972 sind zu vage, um aktuellen Herausforderungen gerecht zu werden. Bisherige Reformversuche blieben erfolglos. Die Gründe dafür reichen von Interessendivergenzen bis hin zu abweichenden Vorstellungen darüber, was Weltraumsicherheit eigentlich umfasst und was nicht. Im Kontext der aktuellen Systemrivalität und der Krise diverser multilateraler Verträge, etwa zur Rüstungskontrolle, ist es unwahrscheinlich, dass diese Differenzen bald überwunden werden können.

Eine Möglichkeit wäre, sich an der Governance des Cyber- und Informationsraums zu orientieren. Statt auf neue, komplexe Vertragswerke setzt man hier eher auf vertrauensbildende Maßnahmen und nichtbindende Normen angemessenen Staatenverhaltens. Zwar scheiterte 2019 eine Group of Governmental Experts der Vereinten Nationen (UNGGE), die sich der Prävention eines Rüstungswettlaufs im Weltraum widmete. Doch einer ähnlichen UNGGE zu Cyber-Sicherheitsfragen gelang es in den letzten Jahren, Konsensberichte zu verabschieden. Die Nachfolgerin dieser Expertengruppe, die Open-ended Working Group, könnte genutzt werden, um etwa eine neue Norm zu verhandeln, wonach Staaten von Cyber-Operationen gegen Weltrauminfrastrukturen abzusehen haben. Zusätzlich sollten die verschiedenen Cyber- und Weltraum-Arbeitsgruppen auf Ebene der UN miteinander in Kontakt treten. Dieser Ansatz hätte den Vorteil, das komplexe Problem der Weltraumsicherheit in einzelne Bestandteile zu zerlegen, wodurch man rein auf die IT-Sicherheitsdimension abzielen und andere Fragen ausklammern könnte. Langfristig ließen sich somit internationale Standards für Cyber-Verhalten im Weltraum definieren und davon ausgehend die weiteren Sicherheitsdimensionen adressieren. Natürlich werden solche Normen zunächst keine starke Bindewirkung entfalten; sie sind daher kein ultimativer Garant für mehr Sicherheit.

Eine andere sinnvolle Maßnahme betrifft den Informationsaustausch über Cyber-Bedrohungen. Derzeit werden in vielen Ländern nationale Zentren für die IT-Weltraumsicherheit gegründet und entsprechende technische Anforderungen festgelegt. Daher wäre es sinnvoll, eine internationale Information-Sharing-Infrastruktur zu etablieren, über die sich einschlägige »best practices« sowie »cyber threat intelligence« austauschen lassen. Sie würde komplementär zum Austausch von konventionellen Bedrohungen über verschiedene Weltraumlagezentren hinweg agieren. Zudem wäre darüber nachzudenken, eigene Computer Emergency Response Teams für Weltrauminfrastrukturen einzurichten, die es bereits für zahlreiche andere Wirtschaftszweige gibt. Weiterhin könnten und sollten die privaten Betreiber von Weltrauminfrastrukturen hier im Sinne von Public-Private Partnerships mit einbezogen werden, wie dies in den USA schon praktiziert wird. Ein zwischenstaatlicher Austausch könnte zunächst unter »like-minded« Staaten, etwa innerhalb der EU oder Nato, stattfinden.

Fazit

Die Domäne Weltraum vermischt sich immer mehr mit dem Cyber- und Informationsraum. Beide sind emergente kritische Infrastrukturen globalen Maßstabs, die keiner staatlichen Hoheit unterliegen und deren Ausfall katastrophale Folgen weltweit haben könnte. Staaten, besonders aber die Europäische Union und ihre Mitglieder sollten hier aktiv werden und entsprechende Mindestanforderungen für Weltrauminfrastrukturen definieren — alle Segmente umfassend. Daraus könnten später internationale Standards erwachsen.

Dr. Matthias Schulze ist Stellvertretender Leiter der Forschungsgruppe Sicherheitspolitik. Der Autor dankt Clémence Poirier, David Fuhr, Daniel Voelsen, Jonas Winkel, Daniel Lambach, Sebastian Harnisch, Frank Christophori und Kim Schuck für wertvolle Impulse.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
DOI: 10.18449/2023A04