War in Space

Was droht dort oben?

JULIANA SÜSS
Sicherheitsexpertin und politische Leiterin für Weltraumsicherheit, Royal United Services Institute (RUSI), London, Moderatorin des Podcasts „War in Space“.

Die von US-Präsident Ronald Reagan 1983 verkündete *Strategic Defence Initiative* (SDI) wurde spöttisch auch als „Star Wars-Programm“ bezeichnet – es ging um die Entwicklung von Raketenabwehrsystemen, die sowohl von der Erde als auch vom Weltraum aus Angriffe abwehren können.[1] Das Programm war nur ein Beispiel, welche Bedeutung der Weltraum im Kalten Krieg für Aufklärungs- und Frühwarnsysteme hatte.

Welche Rolle spielt der Weltraum heute? Hinter dem Stichwort „Weltraumsicherheit“ verbergen sich mehrere Aspekte. Tatsächlich sind die Menschen weltweit heute so abhängig wie nie zuvor von Satelliten, die sich in den

Umlaufbahnen bewegen. Das gilt ebenso für Streitkräfte – durch Nutzung von GPS, Kommunikations- und Aufklärungssystemen – wie auch für die Zivilgesellschaft, denn nicht nur das Navigationssystem im Auto wäre von einem Satellitenausfall im Weltraum betroffen, sondern auch Banküberweisungen und Rettungsdienste. Eine Studie von *London Economics*, einer der führenden spezialisierten Politik- und Wirtschaftsberatungsfirmen in Europa, gab 2017 an, dass ein Ausfall der Satellitensysteme über einen Zeitraum von fünf Tagen allein die Wirtschaft eine Milliarde Britische Pfund pro Tag kosten würde.[2] Die Sicherheit von Weltraumsystemen ist vor allem deshalb wichtig, weil die militärischen Fähigkeiten diese Systeme zu einer potenziellen Zielscheibe machen.

Im Englischen ist das Nachdenken über Weltraumsicherheit durch die verschiedenen Bedeutungen von „safety" und „security" geprägt. Das Stichwort „safety" bezieht sich auf die Sicherheit und den Schutz vor natürlichen Bedrohungen im Weltraum – etwa vor Asteroideneinschlägen oder solarem Wetter, das Satelliten stören kann. Zur „Safety"-Debatte zählt darüber hinaus die Bedrohung durch Weltraumschrott. Die Europäische Weltraumagentur (*European Space Agency*, ESA) schätzt, dass sich 36.000 Teile, die größer als zehn Zentimeter sind, an Weltraumschrott in den Erdumlaufbahnen befinden.[3] Auch kleinere Teile (davon eine Million größer als ein Zentimeter, 130 Millionen kleiner als ein Zentimeter) können bei Kollisionen zu gravierenden Schäden führen. Durch die hohen Geschwindigkeiten in den Umlaufbahnen kann bereits ein Trümmerteil mit einem Durchmesser von nur einem Zentimeter die Einschlagskraft einer Handgranate entwickeln.[4] Die ESA geht von mehr als 640 „break-ups", Explosionen und Kollisionen, die weitere Fragmentierungen ausgelöst haben, aus.[5] So kann eine Kettenreaktion entstehen, die weiteren Weltraumschrott generiert und die Nutzung der Umlaufbahnen zunehmend riskanter macht – in diesem Fall spricht man vom Kessler-Syndrom.

KINETISCHE ANTI-SATELLITEN-WAFFEN

Die Debatte um die Weltraum-„Security" befasst sich hingegen mit menschengemachten Bedrohungen – wie etwa Waffen und Maßnahmen gegen Weltraumsysteme. Was nach Science-Fiction klingt, ist jedoch nicht neu: Nachdem 1957 mit Sputnik der erste Satellit drei Monate lang die Erde umkreist hatte, wurde bereits 1959 die erste Anti-Satelliten-Rakete getestet. Generell können Weltraumwaffen in vier Kategorien eingeteilt werden: kinetisch-physikalisch, nicht kinetisch-physikalisch, elektronisch und cyber.[6]

Die kinetisch-physikalischen Waffen umfassen Anti-Satelliten-Raketen, die von der Erde aus gestartet werden, im All platzierte Projektile sowie Systeme, die Angriffe auf Bodenstationen ausführen. Anti-Satelliten-Raketen,

die von der Erde aus gestartet werden, wurden bereits von den USA, Russland, China und Indien getestet – zuletzt von Russland im November 2021. Die kinetisch-physikalischen Tests verursachen oft große Trümmerfelder, die nur langsam durch die Umlaufbahnen wandern, bis sie in der Atmosphäre verbrennen. So wurde ein Trümmerteil, das bei einem chinesischen Test im Jahr 2007 entstand, vierzehn Jahre später für die Internationale Raumstation ISS zu einem Problem, als sie zur Vermeidung einer Kollision ausweichen musste.[7]

Ko-orbitale Waffen, also Projektile, die im All platziert werden, um von dort aus ihr Ziel zu treffen, sind in der Entwicklungsphase. Es gibt allerdings Beweise, dass Russland Kapazitäten aus dem Kalten Krieg aufleben lässt und diese Technologien in der niedrigen Umlaufbahn testet.[8] Alle kinetisch-physikalischen Tests haben bisher nur eigene, oft ausrangierte Satelliten getroffen. Ein kinetisch-physikalischer Angriff auf einen fremden Satelliten würde eine bisher unangetastete rote Linie überschreiten. Zudem ist diese Art von Angriff schwer zu verstecken oder gar heimlich durchzuführen und ineffizient. Letzteres trifft vor allem auf Satelliten zu, die Teil einer größeren Konstellation sind, da mehrere Satelliten, wenn nicht gar mehrere Hunderte, getroffen werden müssten, um deren Dienste weitgehend zu beeinträchtigen.

„JAMMING“ VON GPS IM KRIEG GEGEN DIE UKRAINE

Zu nicht kinetisch-physikalischen Angriffen gehören unter anderem Nuklearexplosionen, deren elektromagnetischer Impuls Satelliten beeinträchtigt, und das *laser dazzling* („Laserblendung“), das optische Sensoren von Erdbeobachtungs- oder Aufklärungssatelliten blendet, sodass deren Bildaufnahmen unscharf werden. Russland verfügt über solche Laser und hat zudem angekündigt, über eine erweiterte Version des Systems zu verfügen, die durch den Laser Objekte auch kinetisch zerstören kann. Dies kann bisher jedoch nicht belegt werden.[9] Laserblendung ist von der Ausgereiftheit des Weltraumlagebewusstseins abhängig, denn nicht die Stärke des Lasers ist entscheidend (bereits geringe Energie reicht aus), sondern die Fähigkeiten, den angepeilten Satelliten zu verfolgen und zu erfassen. Hinzu kommt, dass der Angreifer nicht feststellen kann, wie erfolgreich die Mission war und ob der Satellit eventuell permanent beeinträchtigt wurde.

Unter elektronischen Gegenmaßnahmen versteht man bereits bewährte Taktiken der modernen Kriegsführung: das *Jamming* und *Spoofing* von Signalen („Stören und Fälschen“). Beim Stören weltraumgestützter Signale können sowohl die Signale zum Satelliten (*Uplink*-Signale) als auch die Signale zur Bodenstation (*Downlink*-Signale) getroffen werden. Das Anpeilen von *Downlink*-Signalen ist jedoch einfacher, da es weniger Energie verbraucht – allerdings muss sich das *Jamming*-System relativ nah an der angepeilten

Bodenstation befinden, um das Signal abfangen zu können. Das *Spoofing*, das Fälschen gesendeter Signale, kann dazu führen, dass Falschinformationen weitergegeben werden. Wir wissen, dass Russland GPS-*Jamming* im Krieg gegen die Ukraine einsetzt.[10]

Weltraumsysteme sind zudem durch Cyberattacken gefährdet, durch die der Angreifer schlimmstenfalls die Kontrolle über einen Satelliten und dessen Steuerung übernehmen könnte. Dass Cyberangriffe technisch möglich sind, bewiesen Hacker bereits zuvor, zum Beispiel im Jahr 2007, als amerikanische Satelliten einer solchen Attacke zum Opfer fielen, nachdem ihre Bodenstation in Norwegen gehackt worden war. In diesem Falle übernahmen die Hacker jedoch nicht die Kontrolle über den Satelliten im All. Die Gefahr der Übernahme eines Satelliten besteht bis heute fort: Eine Studie der Ruhr-Universität Bochum und des Helmholtz-Zentrums für Informationssicherheit aus dem Jahr 2023 ergab, dass die Software kommerzieller Satellitenanbieter verschiedene Schwachstellen aufweist und oft über keine richtigen Mechanismen zum Schutz gegen unbefugten Zugriff verfügt.[11]

DROHT EIN KRIEG DER STERNE?

Die Folgen von Angriffen auf Satelliten wirken sich je nach Nutzung und Art des Angriffs unterschiedlich aus. So ist es möglich, dass Kommunikation und Navigationsdienste temporär unterbrochen werden. Jedoch können auch permanente Schäden entstehen. Staaten haben bereits seit Langem erkannt, dass der Einsatz von Weltraumwaffen weitreichende Folgen haben kann: zum einen das Verursachen von Weltraumschrott, aber auch weitere – etwa potenzielle Fehlberechnungen durch die Störung wichtiger infrastruktureller Satelliten wie Frühwarnsensoren gegen Langstreckenraketen.

Das Verursachen von mehr Weltraumschrott und das Verhindern eines Waffenwettrennens im All wird seit Längerem auch bei den Vereinten Nationen debattiert. Inzwischen haben sich zwei Herangehensweisen herauskristallisiert: zum einen der Top-down-Ansatz, der sich an die Ansätze der Rüstungskontrolle anlehnt und bereits seit 2008 von China und Russland verfolgt wird; zum anderen der Bottom-up-Ansatz, angeführt vom Vereinigten Königreich seit 2020, der versucht, der Herausforderung durch Festlegung „verantwortlicher Verhaltensweisen“ im Weltraum zu begegnen. Durch diese Herangehensweise sollen bestehende Hindernisse, wie die Schwierigkeiten, eine Definition von „Weltraumwaffen“ zu finden, umgangen werden.

Das geopolitische Klima eignet sich momentan nicht, um einen Konsens zwischen den Parteien zu finden – Weltraumsicherheit ist nach wie vor ein politisches Problem, das in Zeiten erhöhter geopolitischer Spannungen kaum gelöst werden kann. Die USA verkündeten 2022 ein Moratorium, das Tests von kinetisch-physikalischen Anti-Satelliten-Raketen verhindern

soll – ein Schritt, dem seitdem mehrere Staaten gefolgt sind, darunter Kanada und alle Mitgliedstaaten der Europäischen Union.

Ein Krieg im All – mit im Weltraum stationierten Waffen, mit kinetischen Explosionen von Satelliten – ist unwahrscheinlich, solange die rationale Motivation besteht, dass man die Erdumlaufbahnen weiterhin für eigene Zwecke benutzen will. Die Kalkulation könnte sich mit der voranschreitenden Entwicklung von kinetisch-physikalischen Waffen, die weniger Weltraumschrott erzeugen, ändern. Der Weltraum ermöglicht zurzeit eine technische Unterstützung für terrestrische Kriege. Ein Angriff auf weltraumgestützte Systeme würde sich entsprechend gestalten: Das Ziel wäre, damit die Fähigkeiten des Gegners auf dem irdischen Schlachtfeld zu beeinträchtigen. Es ist daher weitaus wahrscheinlicher, dass elektronische und Cyberangriffe sowie nicht kinetisch-physikalische Angriffe wie die Laserblendung eingesetzt werden. Das hat auch der Krieg in der Ukraine bestätigt. Es sind deshalb resiliente Systeme, die diesen Angriffen standhalten können, sowie Truppen notwendig, die bereits auf den Ernstfall vorbereitet sind. Dies gilt vor allem für den Fall, dass Weltraumsysteme nicht mehr zugänglich sind und die Navigation ohne GPS und Kommunikation ohne satellitengestützte Systeme funktionieren müssen.

[1] Aaron Bateman: „Keeping the Technological Edge: The Space Arms Race and Anglo-American Relations in the 1980s“, in: Diplomacy & Statecraft, 33. Jg., Nr. 2 / Juni 2022, S. 355–378.

[2] London Economics: Economic impact to the UK of a disruption to GNSS. Showcase Report, April 2017, https://londoneconomics.co.uk/wp-content/uploads/2017/10/LE-IUK-Economic-impact-to-UK-of-a-disruption-to-GNSS-SHOWCASE-PUBLISH-S2C190517.pdf [letzter Zugriff: 25.09.2023].

[3] European Space Agency (ESA): Space debris by the numbers, zuletzt aktualisiert 12.09.2023, www.esa.int/Space_Safety/Space_Debris/Space_debris_by_the_numbers [letzter Zugriff: 25.09.2023].

[4] ESA: cleansat. Space Safety, www.esa.int/Space_Safety/Clean_Space/cleansat#:~:text=Space%20debris%20is%20recognised%20as,grenade%20when%20impacting%20a%20satellite [letzter Zugriff: 25.09.2023].

[5] ESA, zuletzt aktualisiert 12.09.2023, a. a. O., siehe En. 3.

[6] Kari A. Bingen et al.: „Space Threat Assessment 2023“, in: Centre for Strategic and International Studies, April 2023, www.csis.org/analysis/space-threat-assessment-2023 [letzter Zugriff: 25.09.2023].

[7] Joey Roulette: „The space station just dodged debris from a 2007 Chinese weapons test“, in: The New York Times, 10.11.2021, www.nytimes.com/2021/11/10/science/china-debris-space-station.html [letzter Zugriff: 25.09.2023].

[8] Brian Weeden / Victoria Samson (Hrsg.): Global Counterspace Capabilities. An Open Source Assessment, Secure World Foundation, April 2023, https://swfound.org/media/206957/swf_global_counterspace_april2020_es.pdf [letzter Zugriff: 25.09.2023].

[9] Ebd.

[10] Jack Watling et al.: „Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive“, in: Special Report, Royal United Services Institute, 04.09.2023.

[11] Johannes Willbold et al.: Space Odyssey. An Experimental Software Security Analysis of Satellites, Ruhr-Universität Bochum / CISPA Helmholtz Center for Information Security 2023, https://jwillbold.com/paper/willbold2023spaceodyssey.pdf [letzter Zugriff: 25.09.2023].