Weltraummanöver

Schriever Wargame

von Aaron Lye

Der Weltraum ist seit Ende der 50er Jahre des 20. Jahrhunderts militärisch genutztes und umkämpftes Gebiet. Der erste Satellit wurde 1957 von der Sowjetunion in den Orbit befördert. Als Reaktion darauf wurde 1959 von den USA die erste Antisatellitenwaffe erprobt. Seitdem hat die Anzahl der Akteure, die in der Lage sind, Nutzlasten in den Weltraum zu bringen und Satellitensysteme zu betreiben, erheblich zugenommen. Aber auch die Art und Weise, wie Satelliten angegriffen werden, ist diverser geworden. Gleichzeitig hat die Menge an Flugkörpern und Trümmerteilen im Orbit das Risiko von Kollisionen erhöht. Um bestimmte Krisensituationen zu üben, veranstalten Staaten deshalb Weltraummanöver. Ein Beispiel ist das Schriever Wargame der NATO.

Space und Cyberspace

Der Weltraum und der Cyberspace sind getrennte und unterschiedliche Domänen der Kriegsführung mit ihren eigenen (geo-)physikalischen Eigenschaften. Gemein haben sie, dass sie die Grundlage der globalen Kommunikations- und Informationsinfrastruktur sind. Das Funktionieren der Weltwirtschaft als auch militärischer Kommandostrukturen hängt von ihnen ab. Diese Abhängigkeit wächst stetig. Satelliten sind von entscheidender Bedeutung für die militärische Kommunikation und Fernlenkung, Frühwarnsysteme, Überwachung, Aufklärung und Lagebild, Raketenabwehr sowie globale Positionsbestimmung und Navigation via GPS in Echtzeit.[1] Wesentlich für Weltraumoperationen ist die Fähigkeit, Objekte in der Umlaufbahn zu orten und zu identifizieren, was militärisch als Weltraumlagebewusstsein (Space Situational Awareness[2]) bezeichnet wird. Dies erfordert ein globales Netz von Radaranlagen und Sensoren. Folglich sind die Kooperation und der Informationsaustausch beispielsweise innerhalb der NATO üblich. Satelliten, Bodenstationen, Starteinrichtungen, etc. sind entsprechend kritische Infrastrukturen[3], die resilient gegenüber Angriffen gestaltet werden. Ein aktuelles Beispiel ist der informationstechnische Angriff auf das KA-SAT-Netzwerk des amerikanischen Satelliteninternet-Betreibers Viasat am ersten Kriegstag der russischen Invasion in der Ukraine. Ukrainische Behörden bestätigten, dass der Angriff auf den Satelliten KA-SAT-9A zu ernsten Problemen geführt hat.[4] Die Angreifer*innen konnten sich durch einen informationstechnischen Angriff Befugnisse im zentralen Network Operation Center beschaffen. Über diese konnten sie SurfBeam2- und SurfBeam-2+-Modems vieler Endkunden mit kompromittierten Softwareupdates übernehmen und dadurch einen Angriff auf die Verfügbarkeit des Satelliten durchführen.[5]

Attribution von informationstechnischen Angriffen ist bekanntermaßen ein Problem, da Hinweise auf Täter und ihren Ursprung leicht gefälscht werden können. Das trifft z.T. auch für Aktivitäten im Weltraum zu. 2011 gaben US-Militärs zu, dass sie Schwierigkeiten haben, Aktionen im Weltraum zuzuordnen. „Wenn es einen ASAT-Start [Start einer Anti-Satelliten-Rakete] oder etwas Ähnliches gibt, können wir das im Allgemeinen sehen und wissen, was vor sich geht, aber wenn es Objekte in der Umlaufbahn gibt, die vielleicht schon seit Monaten oder Jahren dort sind, können wir ... nicht unbedingt wissen, was ihre Funktion ist. Wie kann man eine Aktion zuordnen, ausgehend davon, was dieses Objekt tut? Das kann sehr schwierig sein.“[6]

Operationen im Weltall wird ein enormes Eskalationspotential zugeschrieben,[7] denn aufgrund der globalen und strategischen Bedeutung von Weltraumressourcen kann ein regionaler Konflikt durch Weltraumoperationen schnell globale Dimension annehmen. Wenn Ressourcen, die in größeren Gebieten einen Dienst bereitstellen, angegriffen werden, um den Dienst in einer bestimmten Region auszuschalten, dann hat das Auswirkungen auf die anderen Regionen des Gebiets. Der Angriff auf KA-SAT-9A veranschaulicht dies. Entsprechend der Netztopologie waren Terminals

in vielen europäischen Staaten (Ukraine, Deutschland, Griechenland, Ungarn und Italien) infiziert. Geräte in Spanien und Portugal waren nicht betroffen. Unter anderem wurde der Betrieb von Tausenden von Windkraftanlagen eingeschränkt. Die Windturbinen liefen zwar noch und erzeugten Strom, aber waren für die Fernüberwachung und -steuerung nicht mehr zugänglich. Dieses hätte als Angriff auf kritische Infrastrukturen und als Kriegsbeitrittsgrund bewertet werden können.

Trotz des enormen Eskalationspotentials ist es üblich, dass Staaten (und nicht-staatliche Akteure) Satelliten und ihre Computernetzwerke angreifen (oder dieses üben).[8] Das Spektrum von Angriffen ist breit.[9] Im Wesentlichen werden folgende vier Typen unterschieden: kinetisch physisch (Detonation eines Sprengkopfes zur Zerstörung eines Satelliten oder einer Bodenstation), nicht-kinetisch physisch (blenden der bildgebenden Sensoren eines Satelliten mittels leistungsstarker Laser), elektrisch (senden von Störsignalen oder falscher Signale) und informationstechnisch (Infiltrierung durch das Ausnutzen einer Sicherheitslücke z.B. in der Software eines Satelliten oder einer Bodenstation). Entsprechend wurden die entwickelten Strukturen der Entscheidungsfindung von der NATO als unzureichend eingestuft. Das Schriever Wargame soll dem entgegenwirken.

Schriever Wargame

Das Schriever Wargame dient der Erforschung kritischer Weltraumfragen, einschließlich der Untersuchung des militärischen Nutzens neuer Weltraumsysteme, der Ermittlung von Lösungen für gemeinsame Herausforderungen und der Förderung der Weltraumunterstützung innerhalb der Luft-, Land-, See-, Weltraum- und Cyberspace-Doktrin.

Obwohl der Weltraum bereits seit Ende der 1950er Jahre und der Cyberspace mit der Entwicklung des ARPANETs seit ca. 1970 militärische Domänen sind und zusammen die Grundlage der globalen Kommunikations- und Informationsinfrastruktur bilden, sind Weltraum- und Cyberspace-Manöver relativ neu. Das jeweils 2-tägige Manöver fand erstmals 2001 statt. Anfangs war es ein Manöver der USA mit 250 Soldat*innen, wenige Jahre später bereits eine gemeinsame Übung von USA, Kanada, dem Vereinigten Königreich und Australien. 2012 wurden Vertreter von sieben weiteren NATO-Staaten (Dänemark, Frankreich, Deutschland, Griechenland, Italien, die Niederlande und die Türkei) zugelassen.[10] Richtig integriert wurden diese NATO-Staaten allerdings nicht. Stattdessen wurden mit Neuseeland die „Five Eyes“ komplettiert. Seit 2016 nehmen Frankreich und Deutschland und seit 2018 Japan ebenfalls teil. Deutschland hat sich 2019 auch der internationalen Combined-Space-Operations-Initiative angeschlossen, der neben den Five-Eyes-Staaten nur noch Frankreich angehört. In ihrem Rahmen soll die Zusammenarbeit in der Operationsführung, Weltraumlage und zum Schutz von kritischen Weltrauminfrastrukturen verbessert werden.[11] Lange führte das Space Innovation and Development Center das Manöver auf der Nellis Air Force Base, Nevada, im Auftrag des U.S. Air Force Space Command, Colorado Springs, durch. Nachdem die NATO sich 2021 für ihr Exzellenzzentrum für Raumfahrt die französische Stadt Toulouse als Standort ausgewählt hat,[12] wurde das Manöver entsprechend in dem Jahr in Frankreich abgehalten.[13]

Geprobt wird ein fiktives globales Szenario, welches Space- und Cyber-Aktivitäten beinhaltet und 10-15 Jahre in der Zukunft spielt. Die Schauplätze des Szanarios variierten in der Vergangenheit (z.B. Horn von Afrika, Europa, Pazifik). Aktuelle Konflikte und Gegner bilden jährlich die Grundlage, die Einzelheiten des eigentlichen Szenarios sind geheim.

Die Ziele des Wargames konzentrierten sich auf die Erkundung der Anforderungen an die Weltraumkontrolle, die Erkundung von Möglichkeiten, den fortgeschrittenen gegnerischen Weltraumfähigkeiten zu begegnen, und die Bewertung der Fähigkeit des Feindes, die eigenen Weltraumfähigkeiten einzuschränken.[14] Ganz konkret geht es beispielsweise um die Erforschung verschiedener kombinierter Führungs- und Kontrollsysteme zum Einsatz und zur Verteidigung von Luft-, Weltraum- und Cyberspace-Fähigkeiten zur Unterstützung globaler und regionaler Operationen; Kriegsführung durch die Kombination von Weltraum- und Cyberspace-Operationen; oder die Förderung des gemeinsamen Verständnisses von Verhalten in der Weltraumdomäne und der Auswirkungen auf die staatliche und koalitionäre Entscheidungsfindung.

Das Szenario umfasste ein ganzes Spektrum von Bedrohungen in unterschiedlichen, domänenübergreifenden Einsatzumgebungen, um zivile und militärische Führungskräfte, Planer und Betreiber von Raumfahrtsystemen sowie die von ihnen eingesetzten Fähigkeiten herauszufordern. Die Teilnehmer*innen befassten sich aber auch mit Raketenstarts und Anti-Satelliten-Bedrohungen von der Erde oder aus dem Orbit. Eines der Hauptziele des Wargames ist es, herauszufinden, wie die verschiedenen Staaten auf derartige Bedrohungen reagieren könnten, da sie oft nicht auf dem gleichen technischen Stand sind oder manchmal nicht über ähnliche Verfahren verfügen, um auf bestimmte Bedrohungen zu reagieren. 2016 wurde beispielsweise ein Szenario eingeführt, bei dem die sieben teilnehmenden Staaten den Zugang zu glaubwürdigen GPS-Informa-

tionen verlieren.[15] Die teilnehmenden sieben Staaten sollten versuchten, auf diese Krise zu reagieren. Es werden aber auch offensive Fähigkeiten trainiert. 2021 trainierten sie beispielsweise Operationen gegen Satelliten fremder Mächte, darunter das Blenden eines gegnerischen Satelliten.

Sowohl strukturell, von den Zielen und Herausforderungen, als auch technisch weisen Weltraummanöver starke Parallelen zu jenen im Cyberspace[16] auf. Das Schriever Wargame scheint eher ein Manöver für die Einübung von Kommandostrukturen zu sein. Konkrete defensive als auch offensive Maßnahmen waren zwar Bestandteil des Manövers, scheinen aber weniger im Fokus zu stehen. Das bedeutet aber nicht, dass diese nicht oder wenig geübt werden. Bekanntermaßen werden offensive Fähigkeiten bei anderen Manövern, wie beispielsweise Space Flag,[17] erprobt. Aufgrund des enormen Eskalationspotentials ist es wichtig zu wissen, wie Militärs in diesen Domänen aufrüsten, üben und operieren.

Anmerkungen

1 Beyza Unal. Cybersecurity of NATO's Space-based Strategic Assets. Chatham House. Juli 2019.

2 Nathaniel Rome. European Militaries Join the U.S. in Space. Georgetown Security Studies Review. 7.4.2021.

3 Union of Concerned Scientists. What Are Satellites Used For? 15.01.2015; Defense Intelligence Agency. Challenges to Security in Space, Januar 2019.

4 Kai Biermann. Ukraine wurde vom Satellitenhack schwer getroffen. Zeit-Online. 16.3.2022.

5 Viasat Corporate. KA-SAT Network cyber attack overview. Viasat.com. 30.3.2022.

6 Robert S. Dudney. Hard Lessons at the Schriever Wargame. Air Force Magazin. 1.2.2011.

7 Ebd

8 Todd Harrison, Kaitlyn Johnson, Makena Young. Space Threat Assessment 2022. CSIS. 4.4.2022; Giacomo Giuliari, Tommaso Ciussani, Adrian Perrig, Ankit Singla. ICARUS: Attacking low Earth orbit satellite networks. USENIX Annual Technical Conference 2021: 317-331.

9 Brian Weeden and Victoria Samson. Global Counterspace Capabilities: An Open Source Assessment. Secure World Foundation, April 2021.

10 Julian Hale. 7 NATO Countries Joined U.S. in Schriever Wargame. Atlantic Organization for Security. 19.4.2012.

11 Andrea Rotter. Sicherheitspolitische Herausforderungen im Weltraum: Handlungsbedarfe und Empfehlungen für Deutschland. Arbeitspapier Sicherheitspolitik Nr. 8/2021. Bundesakademie für Sicherheitspolitik.

12 Das dort entstehende Raumfahrtkommando der französischen Luft- und Raumfahrtwaffe wird das NATO-Kompetenzzentrum beherbergen. Zur Rolle der NATO-Exzellenzzentren siehe u.a.: Christopher Schwitanski: Nato-Exzellenzzentren – Planen für den nächsten Krieg, IMI-Studie 2016/06.

13 Europas erstes Weltraummanöver. german-foreign-policy.com. 15.3.2021.

14 Der Weltraum, die Macht und der Krieg (II). german-foreign-policy.com, 13.10.2021; Lauren Hill. Schriever Wargame Concludes. Schriever Space Force Base. 27.9.2019.

15 Pat Host. Schriever Wargame 2016 Focuses On Loss Of Credible GPS Information. Defense Daily. 6.1.2016.

16 Aaron Lye. NATO-Manöver im Cyberraum: Cyber Coalition, Locked Shields und Crossed Swords. IMI-Analyse, 2022/11.

17 Space Flag ist eine zehntägige Übung der United States Space Force für taktische Raumfahrteinheiten, die sich auf den Einsatz aktueller Fähigkeiten zur Erlangung und Aufrechterhaltung der Überlegenheit sowie Abschreckung und Störung gegnerischer Aktionen im Weltraum konzentriert. Das Ziel des Manövers ist es, den Weltraumstreitkräften ein realistisches, bedrohungsbasiertes Training zu bieten, um ihre Fähigkeit zu verbessern, aktuelle und zukünftige Bedrohungen in einem breiteren Kriegskontext zu analysieren und darauf zu reagieren. Die computergestützten Simulationen umfassten die möglichen Angriffe der vier oben genannten Kategorien (z.B. Abschuss von US-Raketenabwehrsatelliten, das Stören von Satelliten, etc.) Echte Satelliten werden nicht verwendet. Seit 2017 findet Space Flag regelmäßig statt. Zunächst zweimal jährlich, ab 2019 sogar dreimal jährlich. In dem Jahr betrug die Teilnehmer*innenzahl 160 Personen. Darüber hinaus nehmen seit 2019 auch Koalitionspartner aus Australien, Kanada, Großbritannien und den Vereinigten Staaten teil. Cf: Air Force's Space Flag Training Exercise Seeks to Hone Warfighting Skills. Executive Gov. 4.5.2017; Lisa Case. AFSPC makes history with inaugural Space Flag exercise. Air Force Space Command. 25.5.2017; Tom Risen. U.S. Air Force to expand Space Flag satellite war game. Aerospace America. 3.7.2018; Lauren Hill. Space Flag holds first exercise with coalition partners. Air Force Space Command. 25.8.2019.