Cybersicherheit im Weltraum verstehen

Der Cyberraum und der Weltraum haben viel gemein: Sie sind offen, gemeinschaftlich, expansiv, grenzüberschreitend und nicht greifbar. Durch seine Digitalisierung ist der Weltraum immer stärker mit dem Cyberraum verbunden. Diese domänenübergreifenden Verbindungen zu verstehen, ist entscheidend, um die Weltrauminfrastrukturen, von denen die Gesellschaft abhängt, besser zu schützen.

Von Clémence Poirier

Zwei Satelliten im Weltraum vor einem Hintergrund aus Programmiercodezeilen.
Generiert mit DALL-E Open AI

Am 24. Februar 2022 wurde das KA-SAT-Satellitennetzwerk von Viasat, das von den ukrainischen Streitkräften genutzt wurde, Stunden vor Beginn der Invasion der Ukraine Opfer einer gezielten Cyberattacke. Der Angriff sollte in erster Linie verhindern, dass die Ukraine den Weltraum nutzt, um auf die Invasion zu reagieren. Allerdings kam es dadurch zu Auswirkungen in ganz Europa, von denen kritische Infrastrukturen auf dem gesamten Kontinent sowie Tausende ziviler Kunden betroffen waren. Diese Attacke zeigte die Anfälligkeit des Weltraums für Cyberbedrohungen.

Satelliten können genauso wie alle anderen digitalen Objekte gehackt werden. Da die meisten Menschen diese Technologie jedoch im Alltag kaum wahrnehmen, wird schnell übersehen, wie stark Gesellschaften von Satelliten abhängen. Sollte das GPS ausfallen, könnten die finanziellen Verluste allein in den USA rund 1 Milliarde USD pro Tag betragen. Ein Cyberangriff auf einen Satelliten kann zu Störungen auf den Finanzmärkten, im Strassenverkehr, bei Wettervorhersagen, Internetverbindungen und Stromnetzen, sowie bei der Luftsicherung und militärischen Operationen führen.

Die Bedrohung an sich ist nicht neu, doch aufgrund der Digitalisierung von Weltraumsystemen und des Weltraumsektors insgesamt haben die Risiken zugenommen. Satelliten sind heute häufig mit Softwarekomponenten ausgestattet, die mit dem Internet verbunden sind. Zusätzlich setzen die meisten Prozesse bei der Planung, der Herstellung, Tests, dem Start und dem Betrieb der Satelliten auf digitale Technologien. So wurde beispielsweise vor Kurzem die erste Bluetooth-Verbindung zu einem Satelliten in mehr als 600 Kilometern Entfernung hergestellt. Man kann Satelliten daher als teure Computer ansehen, die im Orbit fliegen und wie jedes andere verbundene Gerät auch gehackt werden können. Dadurch hat sich die Angriffsfläche vergrössert. Dies betrifft alle Eingangspunkte, die Angreifer nutzen können, um einen Satelliten zu stören, beschädigen, deaktivieren, oder die Kontrolle über einen Satelliten zu übernehmen.

Die naturgemäss widrigen Bedingungen im Weltraum (z.B. die grosse Entfernung von der Erde, kosmische Strahlen, extreme Temperaturen, radioaktive Strahlung) bringt eine Reihe politischer, rechtlicher, technischer und kommerzieller Herausforderungen in einem Bereich mit sich, der Cyberbedrohungen lange Zeit keine Beachtung geschenkt hat. Darüber hinaus beschränkt sich

die Cybersicherheit von Weltraumsystemen nicht auf die Satelliten in der Umlaufbahn: Sie umfasst auch Lieferketten, die Benutzer- sowie die Boden- und Weltraumsegmente während des gesamtenProduktzykluses. Das macht das Cybersicherheitsproblem im Weltraum sehr komplex.

Diese Analyse betrachtet die Entwicklung des Telekommunikationssektors, die Veränderung der Bedrohungslandschaft im Weltraum sowie die politischen, regulatorischen und kommerziellen Probleme, die diese Entwicklungen mit sich bringen. Abschliessend gibt dieser Artikel einen Ausblick darauf, wie die Schweiz versuchen kann, diese Vulnerabilitäten zu beseitigen.

Militarisierung vs. Bewaffnung des Weltraums

Die Militarisierung des Weltraums beschreibt die Nutzung des Alls für militärische Operationen auf der Erde. Sie begann in den 1950er-Jahren zusammen mit den Fortschritten auf dem Gebiet der ballistischen Raketen und der Atomwaffen. In den 1990er-Jahren fokussierten sich die Diskussionen über die Militarisierung des Weltraums hauptsächlich auf operative Aspekte. Satelliten kamen auf – als wesentliche Ermöglicher militärischer Operationen auf der Erde. Seit 2022 konzentrieren sich die Diskussionen über eine Militarisierung auf die Kommerzialisierung, wobei Kriegsparteien eher auf kommerzielle Dienste als auf militäreigene Systeme vertrauen.

Die Bewaffnung des Weltraums bringt die Positionierung bzw. die Nutzung von Waffen im Weltraum mit sich. Dieses neu aufkommende Phänomen ist bereits latent vorhanden, aber noch nicht eingetreten. Laut dem Weltraumvertrag von 1967 ist zwar der Einsatz von Massenvernichtungswaffen im All verboten, doch das Völkerrecht untersagt den Einsatz von Waffen im Weltraum nicht grundsätzlich.

Domänenverschmelzung

Der Telekommunikationssektor hat sich in den letzten zwanzig Jahren stark verändert und Weltraumsysteme sind heute Bestandteil einer umfassenderen digitalen Infrastruktur. Zwar läuft der Internetverkehr noch immer grösstenteils über Unterseekabel und terrestrischer Glasfasernetze, doch der Anteil des Satelliteninternets ist in den letzten fünf Jahren nach und nach gestiegen. Das liegt an dem Wandel des Marktes für Telekommunikationssatelliten. Dieser setzte in der Vergangenheit auf wenige geostationäre Satelliten, um Übertragungsdienste, darunter Direct-to-Home- und Direktübertragungs-Dienste, zu erbringen. Mit der Kreierung grosser kommerzieller Konstellationen in der erdnahen Erdumlaufbahn ist der Markt zuletzt dazu übergegangen, Breitband-Internetdienste einschliesslich Direct-to-Device-Diensten anzubieten.

Satelliten werden auch zunehmend in die terrestrische Telekommunikation, wie zum Beispiel in 5G- und 6G-Mobilfunknetze, integriert. Man kann davon ausgehen, dass Satelliten für die Internetinfrastruktur weiter an Bedeutung gewinnen werden – nicht nur auf der Erde. Zum Beispiel entwickeln die NASA und die ESA derzeit Standards für das LunaNet, das eine Netzverbindung auf dem Mond sicherstellen soll.

Bedrohungslandschaft

Die Bedrohungslage im Weltraum hat sich verändert. Der Weltraum ist überfüllt: In der Erdumlaufbau befinden sich derzeit etwa 6000 operationelle Satelliten, 100 Millionen Trümmerteile mit einer Grösse von circa 1 Millimeter, 500 000 Trümmerteile mit einer Grösse zwischen 1 und 10 Zentimetern und 30 000 Trümmerteile mit einer Grösse von mehr als 10 Zentimetern. Ausserdem ist im Weltraum ein Konkurrenzkampf entstanden – mit einer steigenden Anzahl an staatlichen und kommerziellen Akteuren. Das All ist daher gleichermassen umkämpft. Die Staaten haben ein breites Spektrum an feindlichen Manövern im Weltraum beobachtet, wie z.B.: Anti-Satellitentests (z.B. China 2007, Indien 2019, Russland 2021), Inspektionsmissionen mit dem Ziel, andere Weltraumressourcen abzufangen, die Freisetzung von Projektilen und den Einsatz hochmanövrierfähiger Raumgleiter sowie neue offensive Haltungen in Militärdoktrinen.

Die Bedrohungslage im Weltraum hat sich ebenfalls verändert. Zu Beginn des Weltraumzeitalters beschränkte sich diese auf elektronische Bedrohungen zwischen sowjetischen und US-Systemen. In den 1980er-Jahren waren es vor allem elektronische Bedrohungen und das Abfangen von Satellitendaten durch Piraten und Amateurhacker sowie die Störung von Satellitenübertragung vor dem Hintergrund des Kalten Krieges. In den 1990er-Jahren führte die Zunahme von Satellitenübertragungen zu einem Anstieg der Satelliten-TV-Piraterie. In den 2000er Jahren kam es häufig zu sogenannten «Spoofings» durch nicht staatliche Akteure sowie durch staatlich finanzierte Angriffe, die grösstenteils auf das Bodensegment abzielten. Seit den 2010er Jahren haben Anzahl und Komplexität der Cyberangriffe weiter zugenommen. Dabei geraten sowohl kommerzielle als auch staatliche Systeme ins Visier einer heterogenen Gruppe von Bedrohungsakteuren.

Heute kennzeichnet sich die Bedrohungslandschaft aus durch ein besseres Verständnis der Abhängigkeit der Gesellschaft und des Militärs vom Weltraum, die Satelliten zu verlockenden Zielen für Bedrohungsakteure macht. Dazu kommt ein Anstieg des Hacktivismus: Zahlreiche Gruppen ergreifen Partei in bewaffneten Konflikten. Kriminelle Gruppen greifen mittlerweile regelmässig Raumfahrtunternehmen an (so attackierte z.B. Lockbit die Firmen SpaceX und Boeing). Bislang haben die Angriffe in der Regel nur temporäre und reversible Auswirkungen verursacht. Inzwischen geht es bei den meisten Vorfällen nicht mehr nur um die Satelliten im Orbit, sondern auch um die Bodenstationen und Endgeräten.

Die Anzahl der Cyberangriffe auf Weltraumsysteme ist zuletzt sprunghaft gestiegen. Allerdings ist es schwierig, exakte Zahlen zu nennen, da die meisten Raumfahrtunternehmen aus dem Verteidigungssektor kamen und von der Annahme ausgingen, Sicherheit durch Unklarheit zu erreichen. Sie vermieden es, Informationen zu teilen, Angriffe zu melden oder Daten über ihre Unternehmen oder Systeme zu veröffentlichen, um eine böswillige Ausnutzung zu verhindern. Ausserdem gab es keine gesetzlichen Verpflichtungen, die es ihnen vorschrieben, Angriffe den Behörden oder Kunden zu melden.

Einige Wissenschaftler und Unternehmen haben versucht die Anzahl der Cyberangriffe auf Weltraumsysteme zu erfassen. Die Ergebnisse veranschaulichen gut wie sich die Bedrohungslage verändert hat. Die Datenbank von Pavur und Martinovic zählt 113 Angriffe zwischen 1957 und 2022. Der Anbieter von Marktinformationen CyberInFlight meldet 337 Cyberangriffe seit den 1970er-Jahren. Davon ereigneten sich 90 im Jahr 2023 und allein 30 im Januar 2024. Abweichungen bei den Zahlen sind auf den Mangel an öffentlichen Informationen und unterschiedliche Methoden zurückzuführen. Darüber hinaus handelt es sich dabei wahrscheinlich um niedrige Schätzungen, da weiterhin viele Angriffe nicht gemeldet werden. Auf nationaler

Ebene weichen Methoden und Daten sogar noch stärker voneinander ab. Die NASA meldete nur im Jahr 2020 1.785 Cybervorfälle (einschliesslich des Verlustes und des Diebstahls von Ausrüstung).

Was ist besonders am Weltraum?

Cyberangriffe auf Weltraumsysteme können – anders als kinetische Bedrohungen – die strategische Stabilität im Weltraum beeinträchtigen. Diese wurde im Laufe der Jahre dank des begrenzten Zugriffs auf Weltraum- und Raumfahrttechnologien sowie aufgrund des eingeschränkten Zugangs zu Anti-Satelliten-Fähigkeiten (ASAT) bewahrt. Ausserdem kann jedes Land, das über Radarfähigkeiten verfügt, kinetische ASAT-Angriffe überwachen und zuordnen, wodurch eine Verschleierung unmöglich ist. Auch verursacht ein kinetischer ASAT-Treffer in der Regel Weltraumschrott, der wahllos andere Satelliten in der Umlaufbahn beeinträchtigt. Cyberbedrohungen stellen einen Paradigmenwechsel dar, denn offensive Cybertools sind relativ leicht zugänglich. Cyberangriffe sind schwer zuzuordnen und können jederzeit glaubhaft abgestritten werden. Cyberangriffe auf Weltraumsysteme verursachen keine Trümmer und wirken sich daher auch nicht nachteilig auf die Angreifer aus – dies kann einen Anreiz für unverantwortliches Verhalten sowohl im Weltraum als auch im Cyberraum sein. Zudem ist der Betrieb vieler kritischer Infrastrukturen von der Satellitenverbindung abhängig. Ein einziger Cyberangriff auf einen Satelliten kann sich auf das Funktionieren mehrerer kritischer Bereiche gleichzeitig auswirken.

Politische Probleme

Bis 2019 hat die Politik es weltweit grösstenteils vernachlässigt, sich mit Cyberbedrohungen für Weltraumsysteme zu beschäftigen. Wissenschaftler haben auf diesen blinden Fleck aufmerksam gemacht und hervorgehoben, dass Cyberrisiken für Weltraumsysteme zu sehr vereinfacht diskutiert und dadurch oftmals missverstanden werden, und dass die Politik im Cyberraum nicht im Einklang steht mit der im Weltraum. Seitdem erkennen die Staaten die Bedrohung zunehmend in ihrer öffentlichen Politik an.

In der Folge haben grosse Weltraumnationen damit begonnen, zusätzlich zu ihrer normalen Weltraumpolitik Weltraumverteidigungsstrategien einzuführen, um auf die sich verändernde Bedrohungslandschaft zu reagieren. 2019 hat Frankreich seine Weltraumverteidigungsstrategie veröffentlicht, die Cyberbedrohungen auf Weltraumsysteme als eine der wahrscheinlichsten Bedrohungen anerkennt. Im selben Jahr hat Italien seine Nationale Sicherheitsstrategie für den Weltraum eingeführt, um auf absichtliche und unabsichtliche Bedrohungen einschliesslich Cyberbedrohungen zu reagieren. Im Jahr 2022 hat Grossbritannien seine Weltraumverteidigungsstrategie verabschiedet, die das schädigende Potenzial von Cyberbedrohungen für die Fähigkeit des Landes, militärische Operationen durchzuführen, betont hat. Darin wurde auch die Entwicklung von Cyberfähigkeiten durch potenzielle Gegner, die britische Weltraumressourcen anvisieren könnten, hervorgehoben. Allerdings beinhalten die meisten dieser Dokumente nur sehr wenig konkrete Vorschläge zur Bekämpfung der Cyberbedrohungen im Weltraum. Frankreich und Italien heben die Einführung offensiver Cyberoperation hervor. Frankreich unterstreicht auch die Härtung von Weltrauminfrastrukturen, sowie den speziellen Aufbau von militärischen Fähigkeiten um ohne Weltraumkomponenten noch operieren zu können. Grossbritannien legt indes den Fokus auf die Einbindung der Weltraumdomäne in bereits vorhandene Cyberübungen.

2020 haben die USA die Space Policy Directive 5 eingeführt, bei der es sich um eine politische Richtlinie handelt, die übergeordnete Grundsätze der Cybersicherheit für Weltraumsysteme festlegt. Die Space-Power-Doktrin der Space Force, der Raumfahrtabteilung der US-Streitkräfte (USSF), unterstreicht, dass Cyberoperationen im Weltall ein wesentlicher Aspekt militärischer Weltraumaktivitäten sind, um die Weltraumdominanz zu bewahren. Dies wird anschliessend in den Grundsatzdokumenten der Space Force sowohl für defensive als auch für offensive Aktionen beschrieben.

Neue Raumfahrtnationen, die über grössere Fähigkeiten im Cyberbereich als in der Raumfahrt verfügen, wie zum Beispiel Estland oder Israel, haben entschieden, Cybersicherheit zu einer Säule ihrer Weltraumpolitik zu machen und sie als Sprungbrett für die Entwicklung ihrer Weltraumprogramme zu nutzen.

Der Cyberangriff auf Viasat vor der Ukraineinvasion war auch ein Weckruf für die politischen Entscheidungsträger in der Europäischen Union. Der Strategische Kompass, die Cyberabwehrpolitik sowie die Weltraumstrategie für Sicherheit und Verteidigung der EU sehen allesamt Cyberbedrohungen für Weltraumsysteme als bedeutend, wahrscheinlich, und schädlich an. Letztere empfiehlt die Implementierung von Security-by-Design, die systematische Integration von Cybersicherheitsstandards, den Austausch von Best Practices unter den kommerziellen Organisationen, die konsistente Sicherheitsüberwachung aller EU-Weltraumprogramme und die Integration von Cybersicherheitsmassnahmen in eine neue Weltraumgesetzgebung.

Regulatorische Probleme

In Europa sind die regulatorischen Rahmen für Cybersicherheit im Weltraum weiterhin begrenzt. Zwar haben elf europäische Staaten ein Weltraumrecht eingeführt, doch keiner von ihnen hat rechtsverbindliche Cybersicherheitsmassnahmen in sein Weltraumrecht integriert.

Auf EU-Ebene hat die NIS2-Richtlinie 2022 anerkannt, dass der Weltraum ein Bereich mit hoher Kritikalität ist und «Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedsstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen,» nötig sind, um strengere Cybersicherheitsmassnahmen sowie Meldemechanismen einzuführen. Allerdings muss die Richtlinie noch in nationales Recht umgesetzt werden, was bislang kaum ein EU-Staat getan hat. Ausserdem gibt es noch Raum für Interpretationen hinsichtlich des Anwendungsbereichs ihrer Umsetzung. Zum Beispiel bei der Frage, ob «Bodeninfrastruktur» auch die Benutzer- und Weltraumsegmente umfasst. Darüber hinaus sind die Massnahmen von NIS2 auch sehr allgemein gehalten und nicht unbedingt auf die Besonderheiten von Weltraumsystemen abgestimmt. Der Sektor wird wahrscheinlich Unterstützung bei der Umsetzung benötigen.

Die EU arbeitet derzeit auch eine Weltraumgesetzgebung aus, von der erwartetet wird, dass sie Cybersicherheitsmassnahmen mit aufnimmt. Parallel dazu beginnen gerade mehrere EU-Mitgliedstaaten, ihre eigenen nationalen Weltraumgesetze dahingehend zu aktualisieren, dass sie Cybersicherheitsmassnahmen mit einschliessen. Doch sie warten zunächst die EU-Gesetzgebung ab.

Es ist wichtig, darauf hinzuweisen, dass die Ausarbeitung spezieller Cybersicherheitsstandards für Weltraumsysteme bislang eher ein langsames und mühseliges Unter-

fangen ist. Herkömmliche Cybersicherheitsstandards sind häufig ungeeignet und berücksichtigen nicht die besondere Natur von Weltraumsystemen und der Orbitumgebung. Einige Organisationen (z.B. das *Consultative Committee for Space Data Systems*) haben erst vor Kurzem spezielle Standards für Weltraumentwicklung ausgearbeitet, die noch innerhalb der Branche eingeführt werden müssen.

Technische Probleme

Cybersicherheit auf der Erde unterscheidet sich von Cybersicherheit im Weltall. Ab dem Zeitpunkt des Starts eines Raumfahrzeugs ist der Zugang zu demselben nicht mehr möglich und es können im Fall von Anfälligkeiten oder Fehlfunktionen auch keine Komponenten mehr entfernt und ersetzt werden. Zwar verspricht In-orbit-Servicing, solche Operationen durchzuführen, doch der Markt ist noch nicht reif. Bei einem Satelliten kann man nicht einfach den Stecker ziehen wie einem Computer auf der Erde.

Die Digitalisierung von Weltraumsystemen erhöht ihre Anfälligkeit für konventionelle Cyberbedrohungen. Das macht die Einführung traditioneller Cybersicherheitsprotokolle erforderlich. Allerdings zeigen die unterschiedlichen Merkmale von Weltraumsystemen auch die Unzulänglichkeit herkömmlicher Cybersicherheitsmassnahmen auf. Beispielsweise ist eine Ende-zu-Ende-VPN-Verschlüsselung, die bei Computern auf der Erde sehr üblich ist, aufgrund ihrer grossen Entfernung von der Erde und dem sich daraus ergebenden Verlust von Datenpaketen für Satelliten nicht geeignet.

Kommerzielle Probleme

In der Industrie wurde das Thema Cybersicherheit lange vernachlässigt, da Betreiber (und Kunden) Latenzzeiten und Effizienz Vorrang vor Sicherheit einräumten. Mittlerweile scheinen die grossen Raumfahrtunternehmen jedoch ein gutes Bewusstsein für Cyberbedrohungen entwickelt zu haben. Schwieriger ist es für Start-ups, die es häufig vorziehen, sich auf die Besonderheiten der jeweiligen Mission zu konzentrieren, oder nicht über die Ressourcen verfügen, Cybersicherheit zu integrieren.

Um Cyberbedrohungen zu begegnen, wurden Brancheninitiativen wie die Space Information Sharing and Analysis Centers (Weltraum-ISACs) ins Leben gerufen, um Informationen über Cyberbedrohungen, Vulnerabilitäten sowie Informationen zwischen Mitgliedern und Regierungsbehörden auszutauschen. Die EU hat 2023 beschlossen, ein Weltraum-ISAC einzurichten. Allerdings wurde noch keine Entscheidung bezüglich der Gouvernanz getroffen. Das gilt auch für die potenzielle Einbindung von Einrichtungen aus Nicht-EU-Staaten wie der Schweiz, Norwegen oder Grossbritannien.

Der Bedarf an Cybersicherheit im Weltraum steigt. Dadurch entsteht ein Markt mit neuen Unternehmen, die sich auf diesen Bereich spezialisiert haben, traditionellen IT-Unternehmen, die versuchen, auf dem Weltraummarkt Fuss zu fassen, und grossen Raumfahrtunternehmen, die daran arbeiten, Dienstleistungen im Bereich Cybersicherheit im Weltraum zu vermarkten. Man geht davon aus, dass diese Branche in den nächsten zehn Jahren Umsätze in Höhe von 33,2 Milliarden USD generieren kann. Das schafft auch Chancen für innovative Länder wie die Schweiz.

Was bedeutet das für die Schweiz?

Wie viele andere europäische Staaten verfügt auch die Schweiz nicht über eigene Satelliten. Dennoch verfolgt die Schweiz Aktivitäten im Weltraum. Infolgedessen ist die Schweiz auch anfällig für Cyberbedrohungen, da mehr als 160 Schweizer Unternehmen an der Weltraumlieferkette beteiligt sind. Verschiedene kritische Wirtschaftssektoren vertrauen auf ausländische Satellitendienste (z.B. der Banken-, Transport- und Logistiksektor sowie die Streitkräfte). Das Funktionieren dieser bedeutenden Branchen hängt daher letztendlich davon ab, dass ausländische Akteure Cybersicherheitsmassnahmen einführen.

Dieser Bereich hat 2021 die Aufmerksamkeit politischer Entscheidungsträger geweckt, die den Bundesrat im Auftrag des Schweizer Parlaments aufgefordert haben, einen Bericht über Cyberrisiken im Weltraum zu erstellen. Im Mai 2024 hat die Sicherheitspolitische Kommission des Nationalrates auf Grundlage der Schlussfolgerungen des Berichts von 2021 einen Antrag eingereicht. Darin wird dem Bundesrat angesichts der wachsenden Bedeutung für die Sicherheitspolitik eine weitere Zusammenarbeit mit der EU im Weltraumbereich empfohlen. Allerdings geht es bei diesem Antrag um den Weltraum im Allgemeinen und nicht speziell um Cybersicherheit im Weltraum.

Auf politischer Ebene ist die Schweizer Weltraumpolitik von 2023 kurz auf die Möglichkeit von Cyberangriffen auf Satelliten eingegangen. Allerdings enthält sie keine Massnahmen zur Sicherstellung der Cybersicherheit des Schweizer Raumfahrtsektors. Auch andere staatliche Politiken behandeln das Thema Cybersicherheit nicht. Was die rechtliche Ebene betrifft: Die Schweiz hat noch kein Weltraumrecht, doch das Land ist derzeit dabei, ein solches zu entwerfen. Es bleibt abzuwarten, ob die Cybersicherheit darin berücksichtigt wird.

Ausblick

Die Bedrohungslandschaft verändert sich. Daher sollten auch das Verständnis von Cyberrisiken sowie die Massnahmen zur Begrenzung dieser Risiken angepasst werden, um die Weltraumressourcen und die umfassenden Dienstleistungen, die sie für die Gesellschaft erbringen, zu schützen. Die neuen Herausforderungen auf dem Gebiet der Cybersicherheit werden darin bestehen, die Lücke bei den Fähigkeiten und Informationen zu schliessen, einen angepassten Rechtsrahmen zu schaffen und herauszufinden, wie man Cyberoperationen im Weltraum am effektivsten durchführt und auf solche reagiert.

Für mehr zur Cybersicherheitspolitik, siehe CSS Themenseite.

Clémence Poirier ist Senior Researcher im Risk and Resilience Team des Center for Security Studies (CSS) an der ETH Zürich.

Die **CSS Analysen zur Sicherheitspolitik** werden herausgegeben vom Center for Security Studies (CSS) der ETH Zürich. Das CSS ist ein Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik. Jeden Monat erscheinen zwei Analysen auf Deutsch, Französisch und Englisch.

Herausgeberin: Névine Schepers
Lektorat: Stefan Soesanto
Layout und Grafiken: Miriam Dahinden-Ganzoni

Feedback und Kommentare: analysen@sipo.gess.ethz.ch
Weitere Ausgaben und Abonnement: www.css.ethz.ch/cssanalysen

ISSN: 2296-0236; DOI: 10.3929/ethz-b-000676388