IKT-Sicherheitskonferenz 2023
Linz/Österreich, am 03.10.-04.10.2023
Raum: **MAIN STAGE**
Vortragdatum/-zeit: **03.10.2023, 12:00-12:25 Uhr**

Zentrum für
Risiko- & Krisenmanagement

Weltraum, Cyber-Sicherheit & Resilienz

Univ.-Prof. Dr. (habil.) Alexander SIEDSCHLAG
Dean & Professor of Homeland Security & Security Studies
College of Arts & Sciences
Worldwide Campus
Embry-Riddle Aeronautical University, USA

EMBRY-RIDDLE
Aeronautical University

EMBRY-RIDDLE Aeronautical University

Überblick

- Aktuelle Beispiele
- Rechtsrahmen für Aktivitäten im Weltraum
- Kritische Infrastruktur und Cybersicherheit des Weltraums – "Old Space"
- Weltraum → Weltraumsysteme und "New Space"
- NIS2-Richtlinie (EU 2022/2555) und ihre Bedeutung für Weltraumsysteme
- Ökosystem der Weltraum-Sicherheitspolitik: Beispiel U.S.A.
- Weltraum-Infrastruktur und Angriffsvektoren
- Methoden zur Störung von Satellitenkommunikation
- Umfassende Satellitenkommunikation: Sowohl Fähigkeit als auch Verwundbarkeit
- Ökosystem-Evolution "New Space"
- Pfeiler weltraumpolitischer Sicherheitsarchitektur
- Strategiebausteine: NATO/PfP, EU, (National) Priorities Framework
- Weltraumpolitische strategische Prioritäten: Sicherheit, Cyber, Resilienz
- Cyberresilienz für den Weltraum
- Technologische "Souveränität" im Weltraum: Beispiel IRIS² (EU)
- Globale Chancen für kleinere und neutrale Staaten

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Weltraum, Cyber und nationale Sicherheit: Ukraine

EMBRY-RIDDLE Aeronautical University

- **Starlink-Angebot des U.S.-Raumfahrtunternehmens SpaceX in Verbindung mit bildgebenden kommerziellen Satellitenfähigkeiten von existenzieller Bedeutung**
- Viasat-Satellitenhack am Vorabend der Invasion komplexer als ursprünglich angenommen
  - ❑ Das Viasat KA-SAT-Network, dass auch Internetzugang für zivile Nutzer in Europa bereitstellt, wurde von der Ukraine zur Streitkräfteführung genutzt
  - ❑ Februar 2022: KA-SAT-Satellitenkommunikationsnetzwerk mit ca. 115,000 Modems und kommerziellen, Regierungs- und Luftfahrtkunden in Europa und Mittlerem Osten
  - ❑ Cyberangriff setzte bis zu 45,000 Modems außer Betrieb
  - ❑ Erst später identifizierte DDOS attack verhinderte, dass die Modems wieder online gingen
- Für den Angriff verwendete "Wiper"-Malware (Zerstörung von Nutzerdaten über die Grenze der Wiederherstellbarkeit hinaus) "Acid Rain" löste z.B. in den USA eine breit gefächerte Behördenreaktion aus
  - ❑ Cybersecurity and Infrastructure Security Agency (CISA) und FBI veröffentlichten Warnungen
  - ❑ National Security Agency (NSA) gab Empfehlungen zum Schutz von Satellitenkommunikation heraus
- NSA hatte im Vorfeld der Ukraine-Invasion Cyberangriffe auf Zulieferer im Verteidigungssektor erwartet, zeigte sich aber von dem Angriff auf einen Satelliten-Internetprovider überrascht

➢ **Notwendigkeit, die "defense industrial base" weiter gefasst zu definieren und zu schützen (über traditionelle "supply chain" hinaus)**

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Weltraumwirtschaft und Katastrophenmanagement

EMBRY-RIDDLE Aeronautical University

- Satellitenbilder und georäumliche Analyse haben die Federal Emergency Management Agency (FEMA) dazu befähigt, genaue Haus-zu-Haus Schadensbewertungen bei Naturkatastrophen vorzunehmen und Unterstützungszahlungen beschleunigt zu leisten
- Diese Alternative zu Vor-Ort-Inspektionen kann nicht nur viel Zeit, sondern auch bis zu 90% der Kosten sparen
- Im Jahr 2021 platzierte die Firma "Planet" 146 Erdbeobachtungs- (EO) Satelliten in niedrigem Orbit; weitere folgten, sodass nun die Fähigkeit besteht, die gesamte Welt alle 24h fortlaufend bildlich zu erfassen
- Neue Chancen für gesellschaftliche Resilienz
- Neue Herausforderungen für Cybersicherheit
  - ❑ Cybersecurity and Infrastructure Security Agency (CISA) arbeitet daran, ihre Empfehlungen zu freiwilliger Satelliten-Cybersicherheit zu konsolidieren
  - ❑ Spezielle Empfehlungen für Kleinunternehmen
  - ❑ Entwicklung frei verfügbarer Onlineressourcen und Empfehlungen zur Absicherung von Weltraumsystem-Netzwerken

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Rechtsrahmen für Aktivitäten im Weltraum

Ausgangspunkt: UN Committee on the Peaceful Uses of Outer Space (COPUOS) (1959)

- **Outer Space Treaty – Weltraumvertrag (1967), 114 Vertragsparteien**
  - ❑ Die Nutzung des Weltraums soll zum Vorteil und im Interesse aller Staaten erfolgen und eine "Provinz" der gesamten Menschheit sein [ähnlich Antarktik-Vertrag von 1961]
  - ❑ Verbot der Stationierung von Massenvernichtungswaffen im Weltraum
  - ❑ Eine nationale Aneignung von Weltraumregionen ist unzulässig (Art. II)
  - ❑ Staaten sind für Weltraumaktivitäten von Regierung als auch Privatwirtschaft verantwortlich und haftbar
  - ❑ Staaten sollen die schädliche Verunreinigung von Weltraum und Himmelskörpern vermeiden
  - ❑ Kein Verbot nationaler Weltraumstreitkräfte (z.B. seit Dezember 2019: U.S. Space Force)
  - ❑ Erlaubnis zur Verwendung militärischer Fähigkeiten zur friedlichen Weltraumnutzung
  - ❑ Offene Fragen z.B. in Bezug auf die Definition "friedlicher" Nutzung: jedwede nichtagressive Nutzung einschließlich Selbstverteidigungsfähigkeiten i.S.v. Art. 51 SVN?
- Nicht erfolgreiches Ansinnen von 8 äquatorialen Staaten in der Erklärung von Bogota (1976), den geostationären Orbit als Naturressource und nicht als Weltraumregion zu definieren, um das Recht auf nationale Kontrolle durchzusetzen
- **Weitere Verträge und Konventionen (Rettung, Registrierung von Flugkörpern u.a.)**
- Abgrenzung nationaler Luftraum (Pariser Konvention 1919) – Weltraum (Weltraumvertrag 1967)
  - ❑ Konventionelle **Kármán-Linie:** 100 km über NN – ab dieser Höhe benötigt ein Flugobjekt Fluchtgeschwindigkeit, um in der Luft zu bleiben
- **Nationale Gesetzgebung**

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Nationale Gesetzgebung Beispiel USA

EMBRY-RIDDLE Aeronautical University

- Office of Commercial Space Operations (1984)
- Gehört nun zur Federal Aviation Administration (FAA)
- Compliance in Bezug auf internationale Verpflichtungen
- Schutz nationaler Interessen
- Public Health und Safety
  → aktuelles Beispiel: Keine Re-entry-Genehmigung für Varda-Experimentierkapsel
- Vorschläge für Anpassungen des nationalen Rechtsrahmens
- Ausbau weltraumbezogener Infrastruktur
- Lizenzierung und Regulierung der privaten Weltraumwirtschaft

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Kritische Infrastruktur und Cybersicherheit des Weltraums: "Old Space"

EMBRY-RIDDLE Aeronautical University

Exemplarische Herausforderungen

- Voraussetzungen für das Greifen des Selbstverteidigungsrechts gem. Art. 51 SVN
- Zurechnung des Angriffs/ der Urheberschaft
- Notwendigkeit und Verhältnismäßigkeit
- Im Falle eines Cyberangriffs kann ein militärischer Gegenschlag nur dann zulässig sein, wenn aktive oder passive Cyberabwehr keine ausreichende Schutzwirkung haben
- Integration von Cyber- und physischer Sicherheit
- Vernetzung staatlicher und privater Akteure

Exemplarischer Lösungsansatz
A Strategic Framework for Space Diplomacy (USA, 2022)

- Erklären der nationalen weltraumbezogenen IKT-Sicherheitsstrategie, weltraumbezogenen Sicherheits- und Resilienzstrategie für kritische Infrastruktur sowie Resilienzstrategie für Weltraumgüter ("space assets")
- Nationale und internationale Cybersicherheits-Interoperabilität
- Sektoren- uns stakeholderübergreifende nationale und internationale Zusammenarbeit zu "best practices" für Risikomanagement
- Internationale Bemühungen zu sicherer und resilienter Infrastruktur

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Weltraum → Weltraumsysteme

EMBRY-RIDDLE Aeronautical University

"Designating space systems—meaning the ecosystem from ground to orbit, including sensors and signals, data and payloads, and critical technologies and supply chains—as a critical infrastructure sector would facilitate a more organized, focused, and coherent approach to risk management, launch authorization, and public-private collaboration. It would signal inside and outside the country that space security and resilience is a U.S. national security priority."

Frank J. Cilluffo and Mark Montgomery, "Time to designate space systems as critical infrastructure," SpaceNews, 14. April 2023, https://spacenews.com/time-to-designate-space-systems-as-critical-infrastructure

Kommerzialisierung des Weltraums ("New Space [Race]")

- Fördert den Trend zur Behandlung des Weltraums als kritische Infrastruktur
- Charakter und Komponenten dieser Infrastruktur?
- Nachhaltigkeit und Resilienz
  - ❑ Fähigkeitsspektrum
  - ❑ "New Space" birgt neue Verwundbarkeiten
  - ❑ "New Space" reduziert aber auch Verwundbarkeiten durch resilienzfördernde Netzwerke vieler kleinerer Satelliten
- Herausforderungen/Grenzen
  - ❑ Starker Fokus auf Funktionalität
  - ❑ Cybersicherheit ist oft ein Nebenprodukt des Versuchs, das Weltraumsystem gegen Ausfälle zu sichern und folgt keiner Risikoanalyse oder Risikoakzeptanzentscheidung
  - ❑ Notwendigkeit einer Zero-Trust-Architektur über das gesamte Spektrum risikobergender Akteure: "hacktivists", Cyberkriminelle, staatliche Akteure und Industriespionage betreibende Wirtschaftskonkurrenten
  - ❑ Integration von szenariogestützter Cybersicherheit in das Management der bereits bestehenden hohen Operationsrisiken

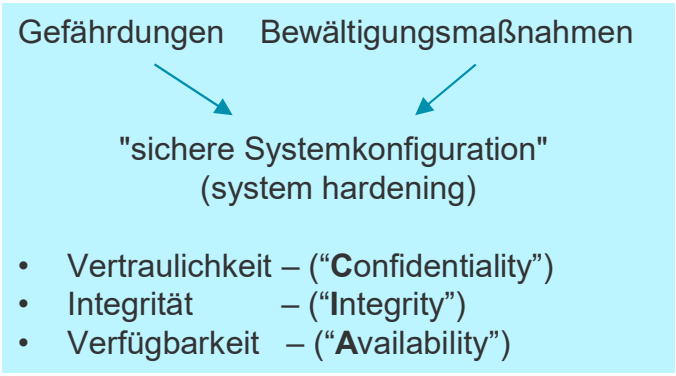
Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

NIS2-Richtlinie (EU 2022/2555)

EMBRY-RIDDLE Aeronautical University

Grundlage: Network and Information Security (NIS) Strategy 2013 als Teil der EU Cyber Security Strategy: An Open, Safe, and Secure Cyberspace

- Schutz kritischer Einrichtungen und die Erhöhung der Widerstandsfähigkeit von Organisationen
- Anwendungsbereich: Unternehmen in EU-Staaten, die in die Kategorien "wesentliche" und "wichtige" Einrichtungen fallen
- Alle betroffenen Unternehmen müssen die NIS2-Richtlinie bis zum 18. Oktober 2024 umsetzen
- Auch Unternehmen, die außerhalb der EU ansässig sind, aber digitale Dienste in Europa anbieten, müssen die Richtlinie möglicherweise einhalten



- ✓ Coordinated Vulnerability Disclosure → **Europäisches Schwachstellenregister (risikobasierter all-hazards-Ansatz)**
- ✓ Meldepflichtigkeit von Angriffen unabhängig von Wirkung/Schadensausmaß
- ✓ Grobbereich innerhalb von 24 Stunden nach Vorfall an jeweilige nationale Behörde
- ✓ Mehr Wissensaustausch und operative Zusammenarbeit zwischen Mitgliedstaaten inkl. EU-Cyber-Krisenmanagement

Bedeutung für Weltraumsysteme

- Neue "wesentliche Einrichtungen" lt. NIS2:
  - ➢ ***Luft- und Raumfahrt***

"Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze"

  - ➢ ***Öffentliche Verwaltung (neu)***
  - ➢ ***IKT-Dienste, einschließlich Cloud Computing Service (neu)***

- Kriterium: Gefahr von Kaskadeneffekten

Ökosystem der Weltraum-Sicherheitspolitik: Beispiel U.S.A.

EMBRY-RIDDLE Aeronautical University

Verschiedene Aspekte von Weltraum als/und kritische Infrastruktur

Strategiefokus? -
Praefix- vs. Suffix-Sicherheitsbegriff
- **Cyber-**Sicherheit oder Cyber-**Sicherheit**?
- **Weltraumsystem-**Resilienz oder Weltraumsystem-**Resilienz**?

Bsp. Space Policy Directive - 5 (U.S.A.)

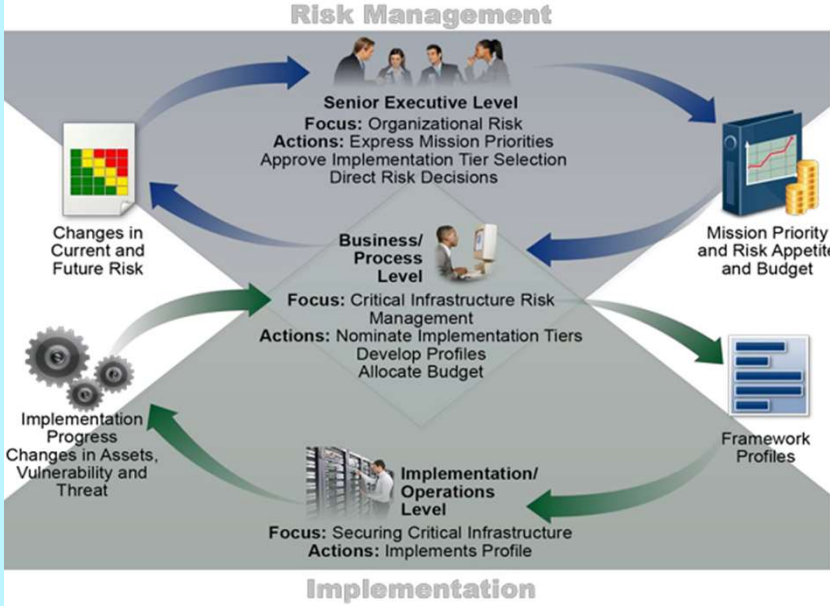
- **Weltraumanwendungen zum Schutz und zur Weiterentwicklung kritischer Infrastruktur**
- **Schutz und Weiterentwicklung weltraumgestützter kritischer Infrastruktur (einschließlich Bodeninfrastruktur)**

FRAMEWORK APPROACH

Zum Beispiel auch ESA: Nutzung der Methodologie nach ISO 27005 (Information Technology – Security Techniques – Information Security Risk Management, 2018)

U.S. Department of Homeland Security Resilience Framework 2018

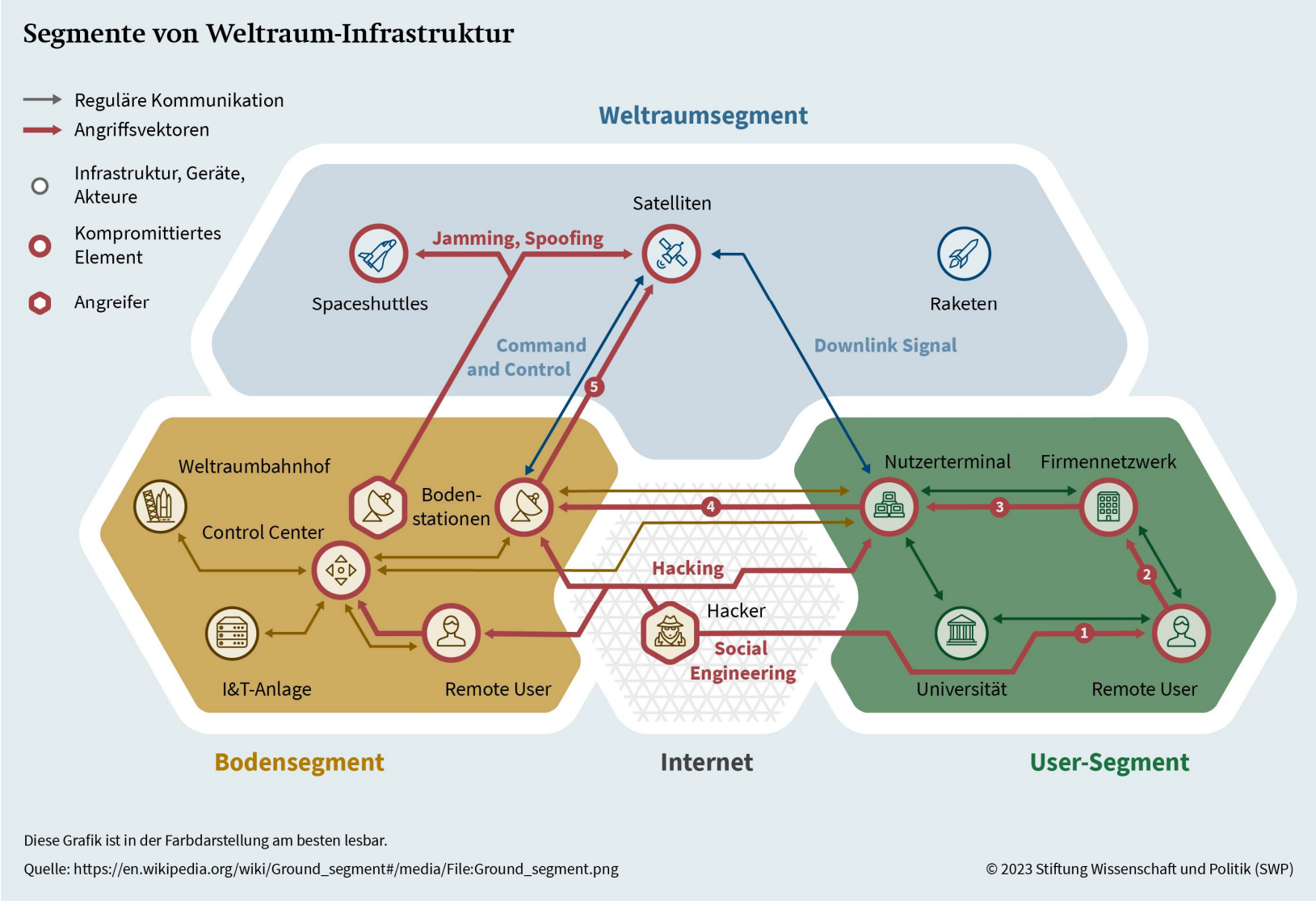
Space Policy Directive – 5 (2020)
- Focussiert/integriert die Zielsetzungen und Maßnahmen der Nationalen Sicherheitsstrategie, der Nationalen Cyberstrategie sowie politischer Richtliniendokumente
- Cybersicherheitsprinzipien und -praktiken beziehen sich sowohl auf terrestrische Systeme als auch auf Weltraumsysteme.
- Integration von Cybersicherheit in alle Entwicklungsphasen von Weltraumsystemen
- Cybersicherheitspraktiken auf der Basis von Präventionskultur, Risikomanagement und geteilter "best practices"



National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 16. April 2018

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Weltraum-Infrastruktur und Angriffsvektoren



- ***Strukturmodell:*** Weltraumsystem als Ökosystem
- ***Schutzparadigma:*** Space-Air-Ground Integrated Network Security (SAGIN)

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Methoden zur Störung von Satellitenkommunikation

EMBRY-RIDDLE Aeronautical University

- **Hacking**
  - ❑ Allgemeine Vorgehensweisen
    - ✓ Distributed Denial of Service (DDOS) Attack auf das SpaceX Starlink-System
    - ✓ Hack-a-Sat-Wettbewerb der U.S. Air Force (s. unten)
- **Saturation**
  - ❑ Bombardieren der Bodenstation oder des Satelliten mit Frequenzvolumen
- **Jamming**
  - ❑ Ablenkung des Kommunikationssignals von der Bodenstation oder dem Satelliten
- **Command Sending (inkl. Spoofing)**
  - ❑ Ersetzen oder Überwältigen des ursprünglichen Signals durch ein Ersatzsignal, das dazu in der Lage ist, den Satelliten in die Irre zu führen
  - ❑ Verschlüsselung muss überwunden werden
- **Zombie Satellites**
  - ❑ Ursachen
    - ✓ Natürliche Ursache: Elektrische Störung durch Weltraumwetter
    - ✓ Bewusste Angriffe
  - ❑ Wirkungen
    - ✓ Kommunikationsausfall
    - ✓ Nicht vertrauenswürdige Daten
  - ❑ Beispiel
    - ✓ Telekommunikationssatellit Galaxy 15 verlor im Jahr 2010 Kommunikation mit der Bodenstation, schickte aber weiterhin Kommunikation an Kunden

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Veranschaulichung: Ethischer Satellitenhack im Wettbewerb

EMBRY-RIDDLE Aeronautical University

Las Vegas, 16. August 2023

- Hack-A-Sat-Wettbewerb
- Organisator: Department of the Air Force (U.S.A.)
- Spezieller Wettbewerbssatellit "Monlighter" (cubesat), von NASA und SpaceX im Juni ins All geschossen
- Satellit hatte nur einige wenige offene Kommunikationsfenster
- Verschiedene Aufgaben ("Challenges")
  - ❑ Z.B. "Weihnachten im August": Moonlighter zum Verlassen seines regulären Orbits bringen und in Richtung Nordpol bewegen
  - ❑ Lösung durch script injection, um den GPS-Empfänger zu täuschen
  - ❑ Z.B "Iron Bank": Satellitenkamera hacken und ein Weltraumfoto machen (s. Bild)

CTF winners mHACKeroni from the Moonlight cubesat (Air Force Research Laboratory)

Realitätsbezug

Chinese National Space Administration (CNSA)

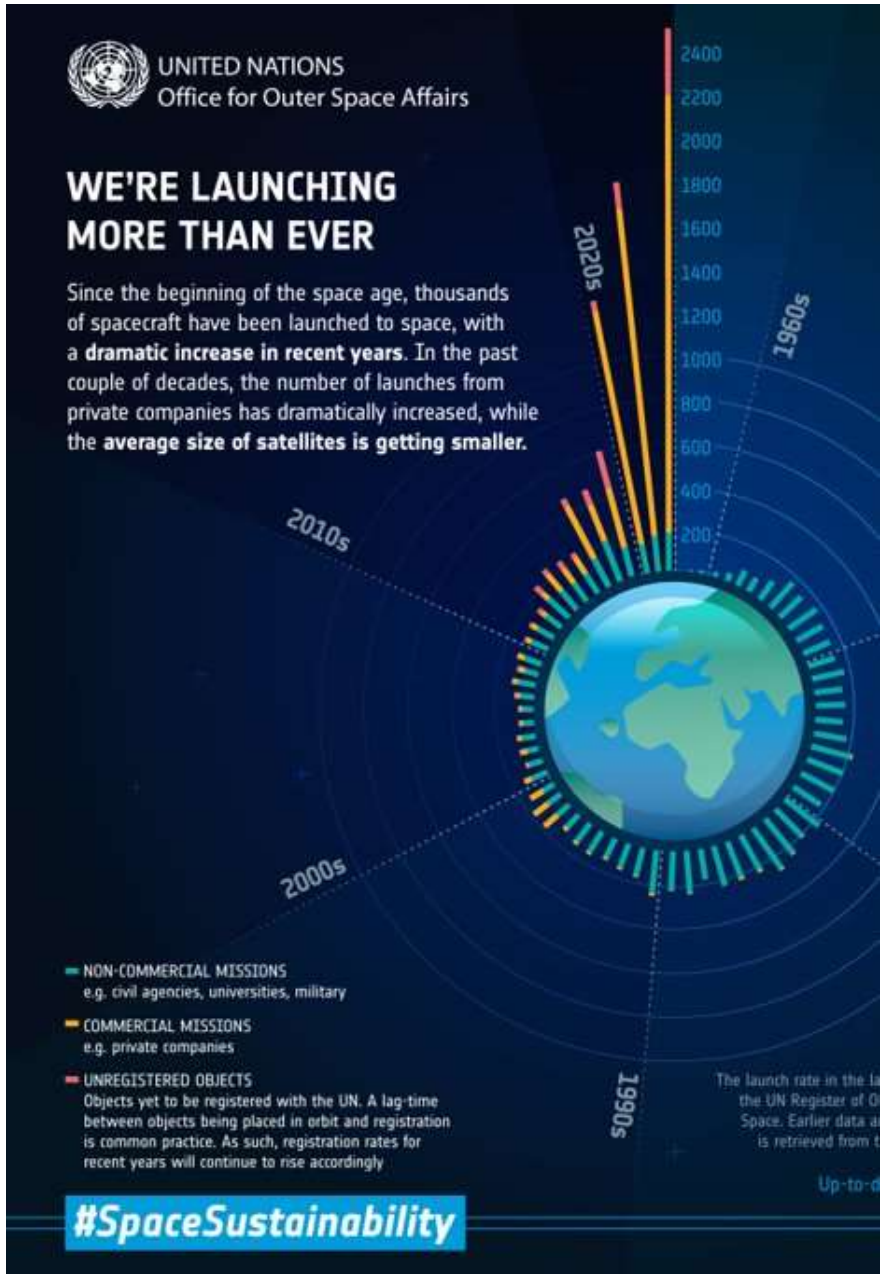
- 2022: 53 Satellitenstarts, 100% Erfolgsquote
- Vermutetes Fähigkeitsziel, die Kontrolle von Satelliten zu übernehmen, um sie in Bezug auf die Unterstützung von Kommunikation, Waffensystemen, Nachrichtendiensten, Überwachung und Aufklärung unwirksam zu machen

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Verwundbarkeiten: Mannigfaltige verknüpfte Angriffsflächen rund um Kommunikation

EMBRY-RIDDLE Aeronautical University

- **“Man kann nicht nicht kommunizieren”**
- Umfassende Satellitenkommunikation: Sowohl Fähigkeit als auch Verwundbarkeit
  - ❑ Erdbeobachtung
  - ❑ Frühwarnung
  - ❑ Navigation
  - ❑ Wettervorhersage
  - ❑ Internetdienstleistungen
    - ✓ von Internetservice für entfernte Weltregionen zu neuer allgemeiner weltraumgestützter Angebotsstruktur)
- Ökosystem-Evolution "New Space"
- Militärische Herausforderung:
  - ❑ Technologische Fortschritte, Änderungen in der strategischen Ausrichtung und neue Sicherheits herausforderungen erfordern Innovationen und Anpassungen, um auf die Durchführung zukünftiger Missionen im, aus dem und in den Weltraum vorbereitet zu sein
  - ❑ Beispiel: "U.S. Space Command actively employs joint forces from the U.S. Army, Marine Corps, Navy, Air Force and Space Force to accomplish the command’s mission"



Ökosystem-Evolution: "New Space"

EMBRY-RIDDLE Aeronautical University

- Zunehmende Relevanz von Weltrauminfrastrukturen mit dem "New Space (Race)"
- Starts ins All: um 2010 rund 130; derzeit rund 2.000; 72 Staaten haben Weltraumprogramme
- Machtverschiebung hin zu privaten Akteuren: das All ist keine nationalstaatliche Domäne mehr
- Viele Weltrauminfrastrukturen sind "dual use": kommerzielle und militärische Dimension (GPS)
- Satelliten der klassischen Ära bringen die für Legacy-Systeme typischen Probleme mit sich:
  - ❑ Ältere, nicht leicht patchbare Software
  - ❑ Wenig Möglichkeiten der nachträglichen Anpassung der IT-Sicherheit im operativen Betrieb im All
  - ❑ Besondere Verwundbarkeit gegenüber Spoofing (Störung der Kommunikation durch manipulierte Signale)
  - ❑ Strategie: Wie können hier die Investitionskosten fuer Hacker erhoeht werden?
- Unternehmen wie SpaceX und Blue Origin suchen die Kosten zu reduzieren, womit die Verwundbarkeiten steigen können:
  - ❑ wiederverwertbare Raketen
  - ❑ günstigere Satellitenproduktion durch Verwendung von Commercial Off-the-Shelf (COTS)-Hardware, Open-Source-Software und neuen Dienstleistungen wie Ground Station as a Service
  - ❑ Damit verbundener Trend zu mehr Software: IT in Weltrauminfrastrukturen immer mehr den gleichen Problemen ausgesetzt wie terrestrische Systeme
  - ❑ Notwendigkeit zukunftsfähiger Satelliten: Angriffsszenarien der nächsten 10-15 Jahre schon bei der Entwicklung antizipieren
  - ❑ Reduzieren hardwareseitiger Schwachstellen, die nicht per Software-Update behoben werden können

RESILIENZ

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Pfeiler weltraumpolitischer Sicherheitsarchitektur

EMBRY-RIDDLE Aeronautical University

UNITED NATIONS
Office for Outer Space Affairs

Beispiel für Zusammenarbeit UNOOSA – ESA: Weltraumschrott (space debris)

- Register of Objects Launched into Outer Space: Identifizierung der verantwortlichen und haftbaren Staaten
- Weltraumgestützte Erdbeobachtungs-fähigkeiten zur Resilienzbildung im Rahmen von Katastrophen-management
- Förderung der Kompatibilität, Interoperabilität und Transparenz zwischen satellitengestützten Informa-tionssystemen
- Nutzung des Weltraums die Sus-tainable Development Goals (SDG)
- Long-Term Sustainability (LTS) of Outer Space Activities
  (Weltraumrecht; Betriebssicherheit von Weltraumoperationen; internationale Zusammenarbeit in der Fähigkeiten-entwicklung; Bewusstseinsbildung)

esa

- **Internationale Organisation**
- Cybersecurity-Initiative:
  - ❑ Relevante Aktivitäten kon-solidieren (threat monitoring, cyber defence, education, etc.)
  - ❑ Technologieentwicklung ein-beziehen: Quantum cryptography, optical communication
  - ❑ Kosteneffiziente Implemen-tierung von Sicherheits-mechanismen durch Stan-dardisierung (z.B. space data link security protocol)
  - ❑ Referenzarchitekturen für Datenverarbeitungssysteme (Weltraum- u. Bodeninfrastr.)
  - ❑ Security by design

EUSPA
European Union Agency for the Space Programme

- **EU-Agentur**
- Betreibt Satelliten-navigationssystem Galileo und European Geostationary Navigation Overlay Service (EGNOS)
- Koordiniert das neue GOVSATCOM-Programm
- Verantwortlich für den Sicherheitslebenszyklus aller Komponenten des EU-Weltraumprogramms
  - ❑ Operational security, security engineering and cybersecurity
  - ❑ Security monitoring
  - ❑ Security accreditation
- Verzögerung bei Ariane-6: ad-hoc security agreement mit den USA, für Galileo-Satelliten

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Strategiebaustein: NATO

EMBRY-RIDDLE Aeronautical University

- Weltraumunterstützung ("space support") durch Mitgliedstaaten oder kommerzielle Dienste, die durch NATO-Agenturen bereitgestellt werden
- ***NATO Overarching Space Policy (2019) und Londoner Erklärung (2019):***
  - ❑ **Weltraum als neuer operativer Bereich der NATO**
    - ➢ Wahrung des Technologievorsprungs
    - ➢ Space Situational Awareness
  - ❑ Koordinierung durch NATO Space Center (eingerichtet 2020 beim Allied Air Command in Ramstein)
- ***Strategisches Konzept der NATO (Madrider Gipfel 2022):***
  - ❑ "enhance our ability to operate effectively in space and cyberspace to prevent, detect, counter and respond to the full spectrum of threats, using all available tools… We will also boost the resilience of the space and cyber capabilities upon which we depend for our collective defence and security."
- ***Gipfel von Vilnius (2023):***
  - ➢ Die **strategische Aufstellung ("posture") der NATO wird ergänzt durch Weltraum- und Cyberfähigkeiten**
  - ➢ Weltraum wird zum **fünften Operationsgebiet der NATO: Cyberspace und Space** sind zunehmend umstrittene ("increasingly contentious") Operationsgebiete, die auf gleicher Höhe wie Land, Luft und Meer angesiedelt sind
  - ➢ Auswirkungen des Weltraumbereichs müssen über alle anderen operativen Bereiche hinweg koordiniert werden
  - ➢ Feindliche Handlungen in den, aus dem oder im Weltraumbereich können zur **Anrufung von Artikel 5** des Nordatlantikvertrags führen

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

NATO Partnerschaft fuer den Frieden (PfP)

EMBRY-RIDDLE Aeronautical University

- **Cyber-Verteidigung ist ein bilateraler Kooperationsbereich**
  - ❑ Cyberbedrohungen sind eine Herausforderung für das Bündnis und seine Partner
  - ❑ Förderung eines freien, offenen, friedlichen und sicheren Cyberspace
  - ❑ Förderung auf internationalem Recht und dem Prinzip der Freiwilligkeit beruhendem verantwortlichem staatlichen Verhalten im Cyberspace
- **Weltraum ist ebenfalls ein bilateraler Kooperationsbereich**
  - ❑ Die NATO erkennt an, dass der Weltraum für ihre Abschreckungs- und Verteidigungsaufstellung ("posture") sowie für ihre zivilen Aktivitäten wesentlich ist
  - ❑ Die NATO erkennt außerdem an, dass der Weltraum überfüllter, strittiger und umrungener wird, und dass einige Akteure Anti-Satellitenfähigkeiten entwickeln, die die Fähigkeit der NATO, im Weltraum zu operieren, herausfordern können
  - ❑ Die NATO strebt danach, ihr Bewusstsein für die Weltraumregion zu erweitern und ihre weltraumgestützten Güter zu schützen sowie verantwortungsvolles Handeln zu fördern
- Die NATO unterstützt ihre Partner dahingehend bei der Entwicklung von Cyber- und Weltraumfähigkeiten durch Maßnahmen wie Ausbildung und Training, Übungen, Informationsaustausch und technische Unterstützung
- Die NATO arbeitet ebenso mit anderen internationalen Institutionen wie EU und UNO and Cyber- und Weltraumfragen gemeinsamen Interesses zusammen

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Strategiebaustein: EU

EMBRY-RIDDLE Aeronautical University

- Weltraum als Faktor der Stärkung der EU als globaler Akteur ***(European Union Global Strategy [EUGS] 2016)***
- Bis vor kurzem keine klare strategische Verbindung von Weltraum und Cyber
- Zugang zum Weltraum entscheidend für die Umsetzung von EU-Politiken

European Union Space Strategy for Security and Defence (März 2023):

- "Europa ist eine globale Weltraummacht"
- Die EU besitzt und betreibt (z.B. im Gegensatz zur NATO) eigene "space assets" für Erdbeobachtung (Copernicus) und Navigation (Galileo)
- Dazu wird das "Union Security Connectivity Programme" (IRIS²) für sichere Kommunikation kommen
- EU Satellitenzentrum: eigene Geospatial-Intelligence-Analysekapazität
- Der Weltraum ist kritisch für die Autonomie der EU und ihrer Mitgliedstaaten
- Einige Weltraummächte haben die Fähigkeit, Weltraum-KI zu bedrohen
- Die EU benötigt eine Weltraum-Abschreckungsstrategie
- Die EU benötigt weltraumbezogene strategische Autonomie
- Die EU muss die Resilienz ihrer space-enabled services for security and defence gewährleisten
- Strategische Integration von Weltraum und Cyber:
  - ❑ EUSPA, CERT-EU, European Union Agency for Cybersecurity (ENISA)

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Strategiebaustein: (National) Priorities Framework

EMBRY-RIDDLE Aeronautical University

Beispiel: The White House, United States Space Priorities Framework (Dezember 2021)

- Schutz weltraumbezogener kritischer Infrastruktur und Stärkung der Sicherheit der **Space Industrial Base**
- Unabhängig von ihrer eigenen Designierung als kritische Infrastruktur aktivieren weltraumgestützte Systeme andere Sektoren kritischer Infrastruktur
- Stärkung der Sicherheit, Cybersicherheit und Resilienz weltraumgestützter System gegen böswillige Handlungen und Naturgefahren in Zusammenarbeit mit der Industrie [vgl. ESA-Ansatz: "Synergien"]
- "Space weather events": Schutz terrestrischer kritischer Infrastruktur mit Schwerpunkt auf Versorgungs- und Lieferketten (supply chain)
- Force Protection: Schutz der Streikräfte vor "space-enabled threats"
- Compliance und Verantwortung: Weltraumoperationen müssen anwendbarem Völkerrecht entsprechen und verantwortlichen Umgang mit der Weltraumumwelt demonstrieren
- Strategie der Abschreckung
  - ❑ Resiliente "space posture"
  - ❑ gestärkte Fähigkeit zur Detektion und Attribution feindseliger Akte im Weltraum
  - ❑ Integration von Fähigkeiten mit Partnern
  - ❑ diplomatisches Engagement mit Gegenspielern
- Investieren in die nächste Generation: STEM education; gesamtgesellschaftlicher Ansatz

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Weltraumpolitische strategische Prioritäten: Sicherheit, Cyber, Resilienz

Inspiriert von: U.S. DOD DIRECTIVE 3100.10 SPACE POLICY, August 30, 2022

EMBRY-RIDDLE Aeronautical University

Sicherheit

- Wahrung der **Handlungsfreiheit** im Weltraum
- Anerkennung des Weltraums als **Wirkungsbereich (domain)** nationaler militärischer Macht
- **Schutz und Verteidigung** der Nutzung des Weltraums für sicherheitspolitische und ökonomische Ziele der eigenen Nation und der Partnerstaaten
- Einbringen weltraumbezogener Fähigkeiten zur **Abschreckung** und Begegnung von Aggression
- Schaffung neuer **Partnerschaften**, die dauerhaften gemeinsamen strategischen Vorteil bieten

Cyber

- Durchführung von Operationen **im, aus dem und in den Weltraum**
- **Unity of effort** / Gesamteinsatz der Fähigkeiten zwischen Behörden und Sektoren, um die Wirksamkeit von Weltraumoperationen und weltraumbezogenen Aktivitäten zu steigern
- Zusammenarbeit mit gleichgesinnten **internationalen Partnern**, um **Normen** für sicheres und verantwortungsvolles Handeln zu etablieren, zu demonstrieren und aufrechtzuerhalten

Resilienz

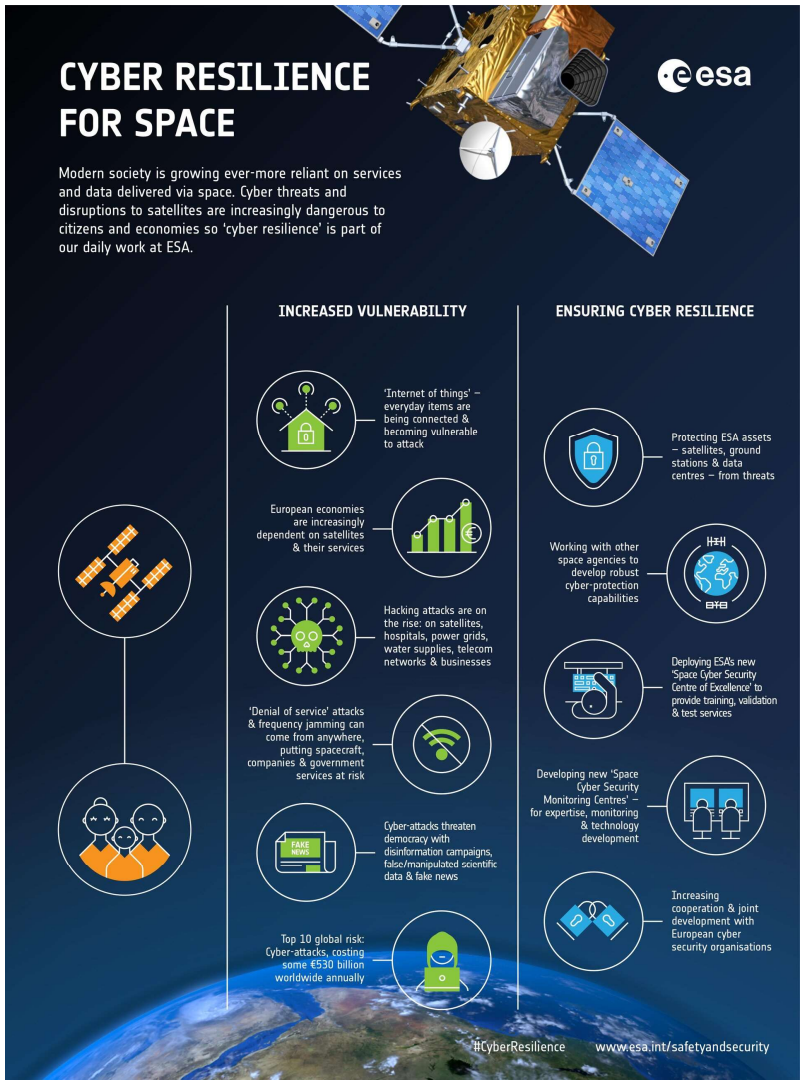
- Stärkung von "safety", "security", "stability", "sustainability" und "accessibility" der **"space domain"**
- Förderung des langfristigen Erhalts der Weltraumumwelt **(Nachhaltigkeit)**
- Nutzen und Fördern einer gedeihenden zivilen und kommerziellen **Weltraumindustrie**, mit wachsender Bedeutung innovativer und entstehender kommerzieller Weltraumfähigkeiten
- **Transformation des nationalen Weltraumsektors**, um anpassungsfähig an raschen Wandel des strategischen Umfelds zu sein

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Cyberresilienz fuer den Weltraum

Referenzdefinition: European Space Agency (ESA), aber fokussiert auf Schließung von Verwundbarkeitslücken in Bezug auf Hacking

- Nutzt aus der Disaster Risk Reduction (UNDRR) bekanntes traditionells risikobezogenes Resilienzkonzept:
  - ❑ **Sicherheitsrisiko** (hazard): v.a. hacking
  - ❑ **Exponiertheit** (exposure): weit verbreitete umfassende/gesamtgesellschaftliche Nutzung von Weltrauminfrastruktur
  - ❑ erhöhte **Verwundbarkeit** (vulnerability)
- Maßnahmen v.a.: Schutz, Monitoring, Zusammenarbeit
- Grenzen des Ansatzes: Fokus auf Verwundbarkeiten kann zu Lasten Anpassungsfähigkeit an veränderte Bedingungen gehen
- Lösungsmöglichkeit: Missionsorientierter Ansatz → **"Operational Resilience Readiness"** (FRAMEWORK APPROACH)
- Weltraum hat darüber hinaus eine weiterreichende Bedeutung für **Resilienz**:
  - ❑ Globaler Zugang zu Information und Kommunikation
  - ❑ Katastrophenmanagement (Erdbeobachung)
  - ❑ Whole-community / societal resilience



Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Technologische "Souveränität" im Weltraum: Beispiel IRIS² (EU)

EMBRY-RIDDLE Aeronautical University

IRIS²: Infrastructure for Resilience, Interconnectivity and Security by Satellite

- Multiorbitale Satellitenkonstellation basierend auf "security by design"
- Soll langfristige Verfügbarkeit von verlässlicher, sicherer und kosteneffizienter Satellitenkommunikation im globalen Maßstab sicherstellen
- Regierungsanwendungen v.a.:
  - ❑ Situationsbewusstsein (z.B. Grenzüberwachung)
  - ❑ Krisenmanagement (z.B. humanitäre Hilfe)
  - ❑ Verbindung und Schutz von Schlüsselinfrastrukturen (z.B. sichere Kommunikation für Botschaften)
- Kommerzielle Massenanwendungen v.a.:
  - ❑ Mobiler and Breitband-Internetzugang durch Kommunikationssatelliten
  - ❑ Satelliten-Trunking für Business-to-Business (B2B)-Anwendungen
  - ❑ Satellitenzugang für den Transportsektor
  - ❑ Verstärkte Netzwerke durch Nutzung auf Breitband und Cloud gestützter Dienste
- Zeitrahmen: Erste Serviceleistungen ab 2024, volle operative Fähigkeit bis 2027
- Technologische Souveränitätsziele:
  - ❑ Robuste und resiliente Kommunikation zwischen Satelliten, die Funksignale mit optischen (lastergestützten) Technologien verbindet
  - ❑ Quantum-Verschlüsselung
  - ❑ Unabhängigkeit von GPS-Satelliten bei Interoperabilität mit EU-Systemen wie Galileo und Copernicus
  - ❑ Skalierbarkeit des Gesamtsystems auf der Basis von User-Analysen (staatliche Organisationen, Industrie, private Haushalte) FRAMEWORK APPROACH
  - ❑ Handhabbarer Umfang (ca. 200 Satelliten)
  - ❑ New Space: Miteinander vernetzte kleinere und billigere Satelliten
- Problem mangelnder europäischer Raketentechnologie und -fähigkeiten, um die benötigten Satelliten in Erdumlauf zu bringen (→ Bedeutung von New Space Startups)

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Globale Chancen für kleinere und neutrale Staaten

EMBRY-RIDDLE Aeronautical University

RESILIENZ

SICHERHEITSKULTUR

- Souveränität und **Selbstverteidigung** erfordern eigene **weltraumbezogene Fähigkeiten**, mindestens gesicherten Zugang zu Satellitenbildern; Fernerkundungsdaten; Kommunikation; Selbst-verteidigungsfähigkeiten gegen erweiterte elektronische Kriegsführung
- **Mindeststandards für IKT-Sicherheit** im Weltraum/in Weltraumsystemen definieren: Internationale Regimebildung - daraus können später internationale Standards erwachsen
- **Ausbildungsoffensive:** Investieren in die nächste Generation: STEM education; gesamtgesellschaftlicher Ansatz
- Weltraumkapazitäten oder Zugang zu diesen entscheidend für **Defense Support of Civil Authorities (DSCA)/"Schutz und Hilfe"**
- Wachsende Bedeutung des Weltraumgebiets in der **Partnerschaft für den Frieden**
- **Cybersicherheit von friedenserhaltenden Einsätzen**

Österreichische Weltraumstrategie 2030+

- Träger der Vision des Weltraums als Allmende (Weltraumvertrag 1967)
- Vorreiter in der Nutzung des Weltraums für umfassende Nachhaltigkeit, insbesondere im Klima- und Umweltschutz
- Standortvorteil als neutraler Hub der internationalen Weltraumpolitik und -diplomatie
- **Kein** Fokus auf **Resilienz** oder **Schutz kritischer Infrastruktur**
- **Rollen/Chancen für nationale New Space Startups**

Vergleich strategischer Weltraumansätze kleinerer und neutraler Staaten
Studie der Air University, 2023

- **Warum?** - Sicherheit, Wirtschaft, Prestige
- **Was?** - Produktion, Nischen-technologie-Spezialisierung, Weltraumdatengewinnung/ -verarbeitung
- **Wie?** - Internationale Koope-ration, international Foren, zivile und militärische Weltraum-agenturen, regionale Schwerpunktbildung (regional hub)
- **Nationales Interesse** – Verbesserter Zugang zu weltraumgestützten Dienstleistungen, gesteigerte Fähigkeit zur Verteidigung nationaler Interessen, Wachstumssektor Weltraumwirtschaft, erhöhte internationale Glaubwürdigkeit

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Globale Chancen: INITIATIVEN

EMBRY-RIDDLE Aeronautical University

- Errichtung eines

  Kompetenz Center: Sicherheitspolitischer Think Tank

  Space Security, Cyber Security, Economical Security, Environmental Security, Societal Security, Political Security und Public Security

  CCSPTT | Competence Center Security Policy Think Tank – Zentrum für Risiko- und Krisenmanagement (zfrk.org)

- **Initiierung und Durchführung der VSSC-Vienna Space Security Conference:** https://www.vssc.at ; https://vssc.space

VSSC 2024
VIENNA SPACE SECURITY CONFERENCE

Save the date!
13.06.-14.06.2024
Vienna

Vergleich strategischer Weltraumansätze kleinerer und neutraler Staaten
Studie der Air University, 2023

- **Warum?** - Sicherheit, Wirtschaft, Prestige
- **Was?** - Produktion, Nischen-technologie-Spezialisierung, Weltraumdatengewinnung/ -verarbeitung
- **Wie?** - Internationale Koope-ration, international Foren, zivile und militärische Weltraum-agenturen, regionale Schwerpunktbildung (regional hub)
- **Nationales Interesse** – Verbesserter Zugang zu weltraumgestützten Dienstleistungen, gesteigerte Fähigkeit zur Verteidigung nationaler Interessen, Wachstumssektor Weltraumwirtschaft, erhöhte internationale Glaubwürdigkeit

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Ausgewählte Literatur

EMBRY-RIDDLE Aeronautical University

Hamilton, J.S. (2020). Practical Aviation and Aerospace Law. 7th ed. Aviation Supplies and Academic, Inc., Newcastle, WA.

Oakley, J.G. (2020). Cybersecurity for Space. Protecting the Final Frontier. Springer, Cham.

Schrogl, K.-U. (ed) (2020). Handbook of Space Security. Springer, Cham.

Schulze, M. (2023). Cyber-Sicherheit im Weltraum. Verwundbarkeiten, Angriffsvektoren und Schutzmaßnahmen. SWP-Aktuell 2023/A 04. https://doi.org/10.18449/2023A04

Simental, A.J., Bynum, T., Holst, J., Cain, W.A. (2021). Space Security. In: Masys, A.J. (ed) Handbook of Security Science. Springer, Cham. https://doi.org/10.1007/978-3-319-51761-2_85-1

Waters, M. (2023). Small States in Space: Space Club Relevancy and National Interest Influence. Journal of Indo-Pacific Affairs (May-June). https://www.airuniversity.af.edu/JIPA/Display/Article/3427964/small-states-in-space-space-club-relevancy-and-national-interest-influence

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich

Kontaktdaten des Vortragenden:

Univ.-Prof. Dr. (habil.)
Alexander SIEDSCHLAG
Präsidiumsmitglied
Zentrum für Risiko- und Krisenmanagement
(ZRK)
Center for Risk and Crises Management (CRC)
A-1030 Vienna, Reisnerstrasse 5/20a, Austria
https://www.zfrk.org
email: alexander.siedschlag@zfrk.org

Zentrum für
Risiko- & Krisenmanagement

Univ.-Prof. Dr. (habil.)
Alexander SIEDSCHLAG
Dean & Professor, College of Arts & Sciences
Embry-Riddle Aeronautical University
Worldwide Campus
32114 Daytona Beach, FL, 1 Aerospace Blvd, USA
https://worldwide.erau.edu/colleges/arts-sciences
email: SIEDSCHA@erau.edu

EMBRY-RIDDLE
Aeronautical University
WORLDWIDE
COLLEGE OF ARTS & SCIENCES

"Innovative Teaching and Research to Foster Positive Global Change"

Presentation supported and sponsored by Zentrum für Risiko- und Krisenmanagement, Wien, Österreich