

Integration der Vorgaben und Richtlinien in die Weltraumprojekte der Zukunft

Miriam Göllner

Cyber Security Engineer Airbus Defence & Space

22.05.2023

Miriam Göllner

M. Sc. Information Systems Management

@ Technische Universität Berlin

Background in Cyber Security

Verschiedene Kurse in Cyber Security im Masterstudium belegt (2017 – 2020)

Werkstudentin am IT-Dienstleistungszentrum Berlin im Bereich Security & Compliance (2018 – 2019)

Rolle Cyber Security Engineer

@ Airbus Defence & Space Cyber Programmes

Tätig im Bereich Space Systems Security

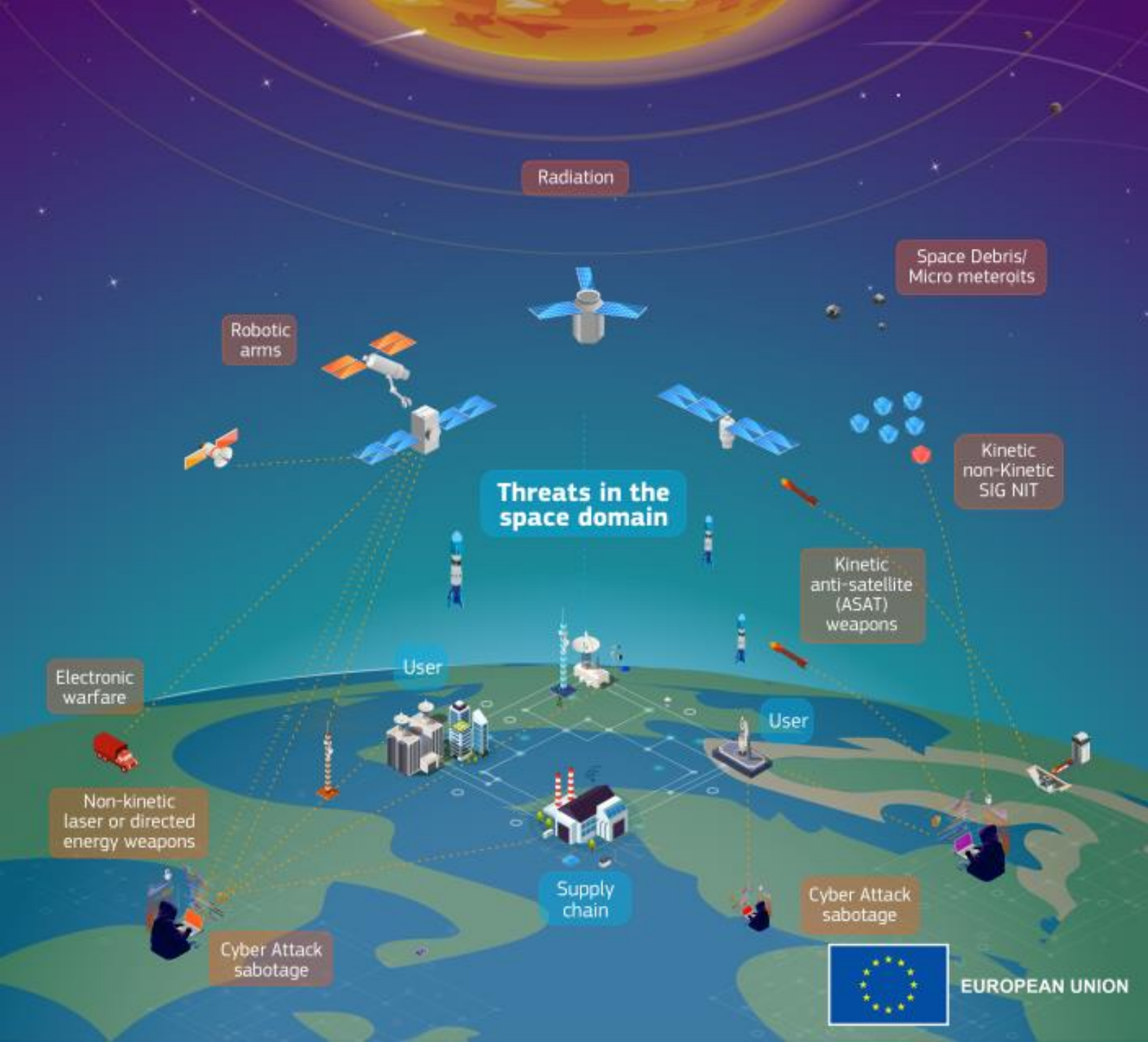
Fokus liegt auf militärischen Missionen

Zertifizierte BSI IT-Grundschatz Praktikerin

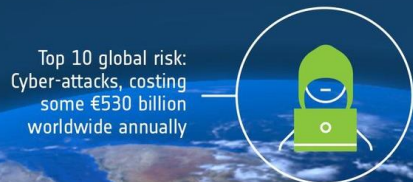
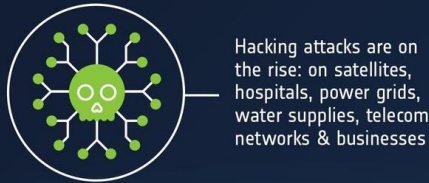
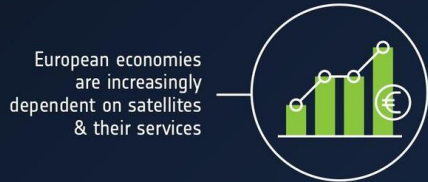
Bedrohungen für Weltrauminfrastrukturen

- Bedrohungen haben Einfluss auf das Raumsegment, das Linksegment und die Bodeninfrastruktur
- Cyber Security Bedrohungen sind ein Teil der Bedrohungen für Weltrauminfrastrukturen
- Cyber Security Risiken müssen im Lebenszyklus des Satelliten identifiziert werden

Source: <https://defence-industry-space.ec.europa.eu/system/files/2023-03/Infographics%20-%20Threats%20in%20the%20space%20domain.pdf>



INCREASED VULNERABILITY



ENSURING CYBER RESILIENCE



Cyber Resilienz

Zunehmende Verwundbarkeit

Steigende Anzahl an Schwachstellen durch IoT, Abhängigkeit von Satelliten Services, zunehmende Hacking Attacken/ DoS Attacken, Bedrohung der politischen Lage, Teil der Top 10 globalen Risiken

Cyber Resilienz schaffen

Schutz der Assets, Kollaboration verschiedener Organisationen, Entwicklung von Space Security Operations Centres, gemeinsame Entwicklung neuer Lösungen

Source: https://www.esa.int/Space_Safety/Cyber_resilience

Standardisierter Schutz vor Bedrohungen auf Basis von Vorgaben/ Richtlinien

Einheitliches Schutzniveau

für kommerzielle und militärische Missionen

Einheitliche interne und externe Vorgaben

Anwendung einheitlicher Rahmenwerke für Missionen

Nachweisbarer Schutz in den Lieferketten

Adressieren der Vielzahl an Schwachstellen

Moderne Informationssicherheitsvorgaben

Vorgaben basieren auf modernisiertem BSI IT-Grundschutz

Teilen von Cyber Threat Intelligence

Kollaborationsvorhaben verschiedener Organisationen

Zukünftige Weltraumprojekte

Satellitenkommunikationssysteme

Störungen und Interferenzen - absichtlicher oder versehentlicher Art – waren schon immer ein Problem für die Satellitenkommunikation. Ihre Zunahme erfordert effektive Gegenmaßnahmen, um sicherzustellen, dass geschäftskritische Konnektivität jederzeit und in allen Situationen belastbar, ausfallsicher und geschützt vorhanden ist.

Einige der weltweit sichersten militärischen Netzwerkmanagementsysteme wurden von Airbus entwickelt und geliefert, darunter das britische System Skynet 5, das deutsche System SATCOMBw und das System von Yahsat.



Source: <https://securecommunications.airbus.com/de/systeme/satcom-networks>; <https://strategie-technik.blogspot.com/2016/03/anschlussauftrag-airbus-betreibt.html>

Zukünftige Weltraumprojekte

Navigation

EGNOS verbessert die Genauigkeit von Satellitennavigationssystemen wie dem europäischen Galileo oder dem US-amerikanischen GPS und sichert gleichzeitig die Verlässlichkeit der Daten.

EGNOS V3 soll in mehreren Stufen zwischen 2023 und 2025 in Dienst gestellt werden, um das europäische System noch genauer, robuster und besser verfügbar zu machen. Auch der Schutz vor Cyberattacken wird verbessert.

Neben EGNOS entwickelt Airbus auch die zweite Generation der Satelliten des europäischen Navigationssystems Galileo.



Source: <https://www.airbus.com/en/products-services/space/navigation>;
<https://www.airbus.com/en/newsroom/press-releases/2022-12-airbus-achieves-key-milestone-on-egnos-european-satellite-based>

Zukünftige Weltraumprojekte

Erdbeobachtung

Scharfe Augen im All - optische
Satellitenkonstellation Pléiades Neo

(Foto der Engelsburg in Rom mit 30
Zentimetern Auflösung,
aufgenommen von einem neuen
Pléiades-Satelliten im Mai 2021)



Source: <https://www.sueddeutsche.de/wirtschaft/raumfahrt-airbus-erdbeobachtung-1.5422999>