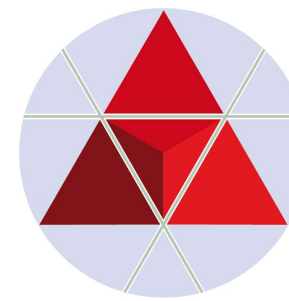


# LEADERSHIP PREPAREDNESS SYMPOSIUM

WITH KEYNOTE PERSONALITIES FROM THE NPLI



Zentrum für  
Risiko- & Krisenmanagement



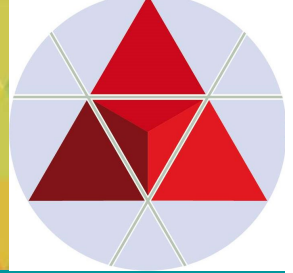
Interactive Session 8: Trade and Technology Innovation:

## “Critical CYBER and SPACE infrastructure risks for the supply and value chain”

Johannes GOELLNER, 22.05.2024, 3:05-4:00 pm

excellent.  
connected.  
individual.

# Press releases: SPACE



Was kostet es, den besten Tarif zu haben? **JETZT WECHSELN**  
Anmeldung bis 14.01.2024 - 07.01.2024  
\*Details auf www.eth.comcast.it

**Geschäft mit dem Weltraum wird zur 1,25-Billionen-Euro-Chance**  
Aerospace, Konsum oder Energie: Raumfahrtstechnologie eröffnet laut einer neuen Studie riesige Märkte für die deutsche Industrie – „vergleichbar mit China“.  
Thomas Jahn  
17.10.2023 - 18:26 Uhr

**Ehemaliger NASA-Forschungschef kommt an die ETH Zürich**  
Von 2016 bis 2022 hat Thomas Zurbuchen die Forschung der Weltraumbehörde NASA verantwortet. Ab August übernimmt er die Leitung der ETH Zürich Space. Mit dieser Initiative soll die Raumforschung und -lehre an der ETH ausgebaut und die Zusammenarbeit mit der Raumfahrt-Industrie gestärkt werden.

**US-Behörde verhängt Strafe gegen Satellitenbetreiber**  
Ein stillgelegter Satellit muss dorthin gebracht werden, wo er keine Gefahr stellt. Ein Betreiber muss Strafe zahlen, weil er dem nicht nachgekommen ist.  
5. Oktober 2023, 11:31 Uhr, Werner Pluta

**Ausflug ins All für Österreichs ersten Weltraumtouristen**  
Der Waldviertler Franz Haider verließ als erst zweiter Österreicher in der Geschichte die Erde – mehr als fünf Jahrzehnte, nachdem Neil Armstrong den Traum in ihm geweckt hatte.

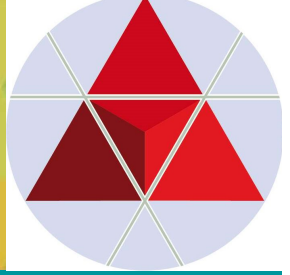


Franz Haider zeigt es an: Am Freitag ging es für ihn ins All



Satelliten im Orbit (Symbolbild): Die FCC hat Regeln zum De-Orbiting erlassen.

# Press releases: SUPPLY CHAIN & CYBER



[Zurück](#)

Dienstag, 09.04.2024

Seite 2 von 28

2 RESILIENZ contentway

RESILIENZ



AUSGABE #151

Campaign Manager:  
Marin Nam „Marin“ Nguyen

Geschäftsführung:  
Nicole Bitkin

Head of Content & Media Production:  
Aileen Reese

Redaktion und Grafik:  
Aileen Reese, Nadine Wagner,  
Dennis Wondruschka, Miguel Daberkow

Text:  
Sija Ahlemeyer, Armin Fuhrer, Jörg Wernien,  
Katja Deutsch, Jakob Bratsch, Nadine  
Wagner, Thomas Soltau, Julia Butz

Coverfoto:  
Shutterstock, Presse/Frosta, Pexels

WEITERE INHALTE

- 4. Hannover Messe 2024
- 6. Digitale Resilienz
- 8. Prof. Dr. Eckert
- 14. Felix Ahlers
- 16. Marcus Diekmann
- 18. Weltwirtschaftsforum (WEF)
- 24. Supply Chain
- 26. Cawa Younosi

CONTENTWAY.DE

## Cybersicherheit hat höchste Priorität

Das Bundesamt für Sicherheit in der Informationstechnik schätzt die IT-Sicherheitslage in Deutschland als angespannt bis kritisch ein. Im Schnitt wurden im Zeitraum von Juni 2020 bis Mai 2021 täglich 394.000 neue Schadssoftware-Varianten bekannt.

## Resilienz ist mehr als Krisenmanagement

EINLEITUNG

Seit einigen Jahren werden Unternehmen durch multiple Krisen herausgefordert: Naturkatastrophen, kriegerische Auseinandersetzungen, Klimawandel, politische und gesellschaftliche Veränderungen, zunehmende Regularien, die ökonomischen Herausforderungen eines angespannten Marktes sowie disruptive Technologien.

Foto: Presse



Tanja Kruse-Jones,  
Director Supplier Management EMEA  
bei ISG Germany GmbH

Dienstag, 09.04.2024

Seite 6 von 28

[Zurück](#)

Dienstag 9. Apr.

[Zurück](#)

Dienstag, 09.04.2024

Seite 8 von 28

8 RESILIENZ contentway

## Unternehmen müssen damit beginnen, vertrauenswürdige Cyberresilienz zu etablieren

KÜNSTLICHE INTELLIGENZ

Die Digitalisierung der Welt schreitet in Riesenschritten voran. Mehr denn je müssen wir daher Angriffe auf unsere IT nicht nur bestmöglich verhindern, sondern die, die erfolgreich sind, auch frühzeitig erkennen, um darauf reagieren zu können. Alle dafür erforderlichen Maßnahmen dürfen ihrerseits nicht von Angriffen unterwandert werden können. Die Etablierung einer solchen „vertrauenswürdigen Cyberresilienz“ geht deshalb deutlich über den Zero-Trust-Ansatz hinaus.



Prof. Dr. Claudia Eckert,  
geschäftsführende Leiterin  
des Fraunhofer-Instituts

helfen, Sicherheitsauflagen individuell, angemessen und audierbar umzusetzen. Das Fraunhofer AISEC ist eine solche Organisation. Beispielsweise führen wir automatisierte Risikoanalysen durch, entwickeln dann Konzepte, um die Risiken zu minimieren und begleiten bei deren Umsetzung.

Warum ist angewandte Cybersicherheit wichtig?

Dienstag, 09.04.2024

Seite 17 von 28

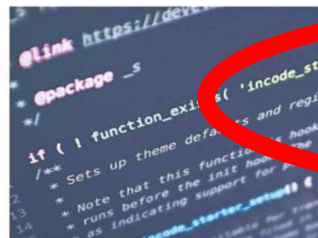
6 RESILIENZ contentway

## Digitale Resilienz

INTEGRATION NEUER TECHNOLOGIEN

Durch digitale Technologien widerstandsfähiger werden. IT als Enabler zukunftsfähiger Business-Modelle.

Text: Julia Butz  
Foto: Luca Bravo/unsplash



## NIS2: Europas Schutzschild gegen Cyberkriminalität

Ab Oktober 2024 müssen alle Unternehmen mit mindestens 50 Mitarbeitern und einem Umsatz Cybersicherheitsmaßnahmen der NIS2-Richtlinie umsetzen. Diese Vorgabe betrifft Unternehmen aus 18 verschiedenen Sektoren. NIS2 ist ein wichtiger Schritt gegen die zunehmende Cyberkriminalität, denn wäre diese Cyberkriminalität ein Staat, würde er – gemessen an seinem Bruttoinlandsprodukt – zu einem der 15 größten Staaten der Welt zählen.

... auch Länder finanzieren

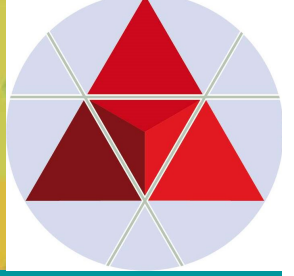
view über mögliche Angriffsszenarien und Unterstützung der IT.  
**Herr Köhne, was sind die häufigsten Angriffe auf IT-Unternehmen in Deutschland?**  
Am häufigsten sind nach wie vor Ransomware-Angriffe, bei denen die Systeme und Daten der Opfer verschlüsselt werden. Im Anschluss werden dann Lösegeldforderungen gestellt. Doch es ist fraglich, ob das Entschlüsseln der Daten nach einer Zahlung funktioniert. Oft wird auch mit der Veröffentlichung sensibler Kundendaten gedroht. Die Opfer müssen ihr gesamtes IT-System komplett neu aufsetzen. Wer das nicht tut, läuft

jedoch erwähnt werden, dass es noch diverse weitere Cybergefahren gibt. Besonders relevant ist vor allem die zunehmende Nutzung von KI durch die Angreifer, z. B. für Phishing Attacken.  
**Weshalb bekommen viele Unternehmen ihre IT-Probleme selbst so schwer in den Griff?**  
Oft gibt die Geschäftsführung kaum Budget frei, da sie keinen Bedarf für mehr IT-Security sieht. Doch es geht nicht mehr darum, ob man angegriffen wird, sondern wann. Zudem sehen wir häufig Mängel im Schwachstellenmanagement und bei der Vergabe von privilegierten Rechten im IT-Bereich. Auch den Einsatz



Ingo Köhne,  
Geschäftsführer IT-Consulting  
bei Möhrle Happ Luther

formal Informationssicherheit umsetzen. Mit DORA haben wir noch eine weitere Verordnung, der Digital Operational Resilience Act tritt im Januar 2025 in Kraft. Er betrifft das gesamte Finanzumfeld. Wir unterstützen die Unternehmen



## Commercialization of space ("New Space")

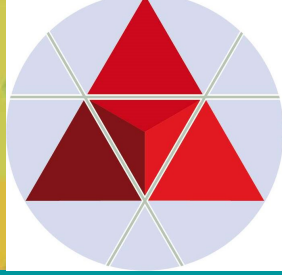
- Promotes the trend toward treating space as critical infrastructure
- Character and components of this infrastructure?
- Sustainability and resilience
- **Fähigkeitsspektrum**
  - ❑ **"New Space" harbors new vulnerabilities**
  - ❑ **"New Space" but also reduces vulnerabilities through resilience-promoting networks of many smaller satellites**

**“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.]”** Source: Frank J. Cilluffo and Mark Montgomery, *"Time to designate space systems as critical infrastructure,"*

*Space News*, 14. April 2023, <https://spacenews.com/time-to-designate-space-systems-as-critical-infrastructure>

# Overview: Statistics (2023)

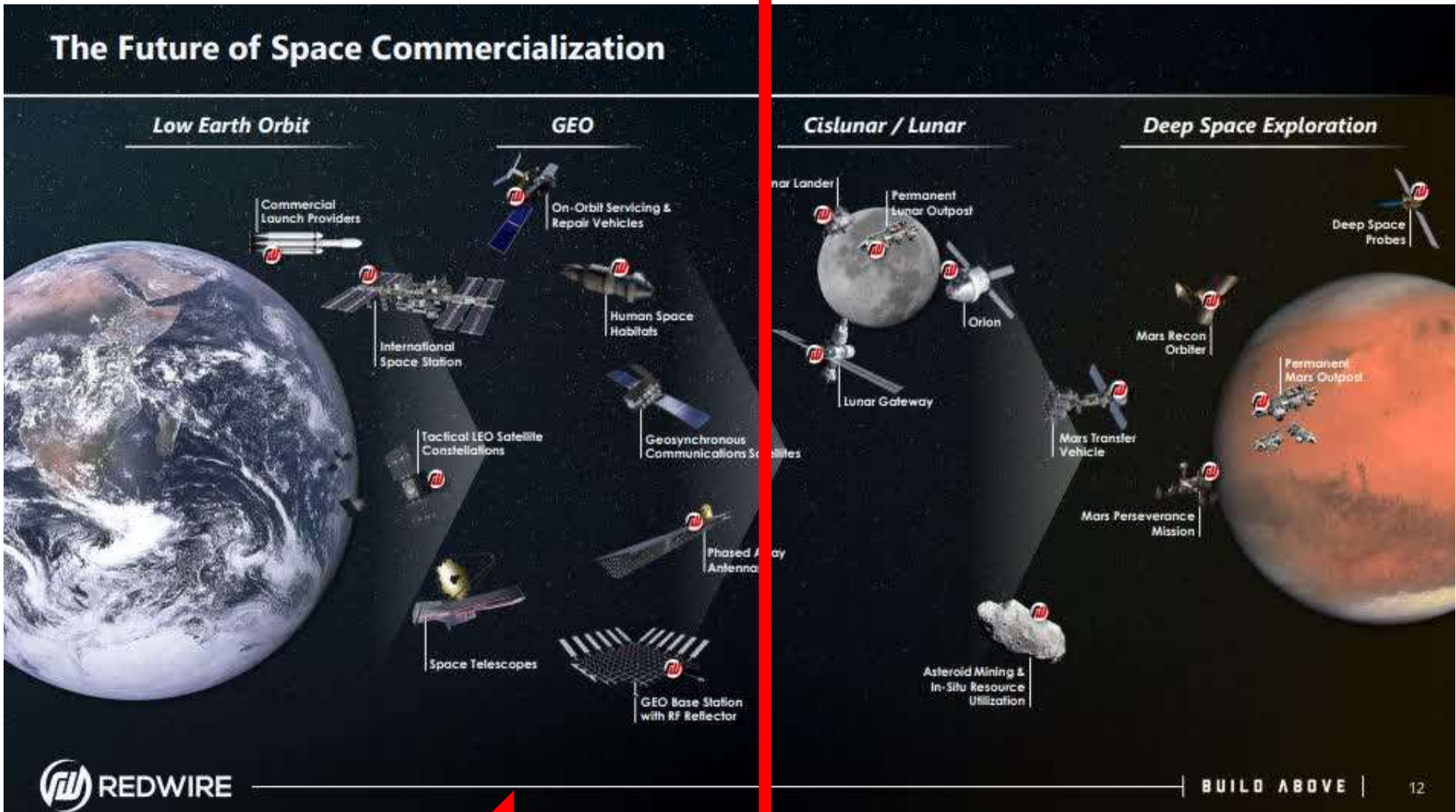
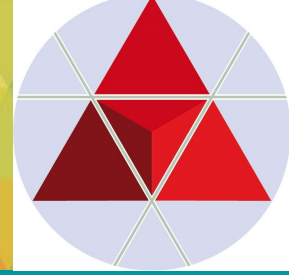
- worldwide % ( +AT; +GE; +CH;)



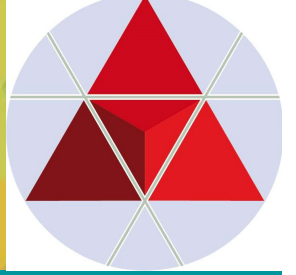
## The 10 largest global business risks in 2023

- 1. Cyber Events: 34%** (AT: 40%; GE: 40%; CH: 57%)
- 2. Supply Chain Interruption-Betriebsunterbrechung: 34%**  
(AT: 32%; GE: 46%; CH: 41%))
- 3. Makroökonomische Veränderungen: 25%* (AT: 24%; GE: 17%; CH: 14%))
- 4. Energiekrise/Energy Crises: 22%** (AT: 38%; GE: 32%; CH: 48%))
- 5. Rechtliche Veränderungen: 19%* (AT: 14%; GE: 23%; CH: 18%))
- 6. Natural Disaster: 19%* (AT: 22%; GE: 19%; CH: 18%))
- 7. Klimawandel: 17%* (AT: 16%; GE: 17%; CH: 9%))
- 8. Fachkräftemangel: 14%* (AT: 24%; GE: 17%; CH: 16%))
- 9. Feuer, Explosion: 14%* (AT: 20%; GE: 13%; CH: *k.A.%*)
- 10. Politische Risiken: 13%* (AT: *k.A.%*; GE: *k.A.%*; CH: 20%))  
*Kritische Infra (Stromausfälle,..): k.A.%* (AT: 22%; GE: 13%; CH: 11%))

# Terrestrial & Space Infrastructure (SUPPLY CHAIN NETWORK)



# Terrestrial & Space Infrastructure (SUPPLY CHAIN NETWORK)



## Space integrated computing network

Independent, carbon-free, autonomous space infrastructure unaffected by disasters on earth  
Ultra-low-power, ultra-high-speed, high-security network achieved by optical technology

Activity area

↑

Moon  
380,000 km

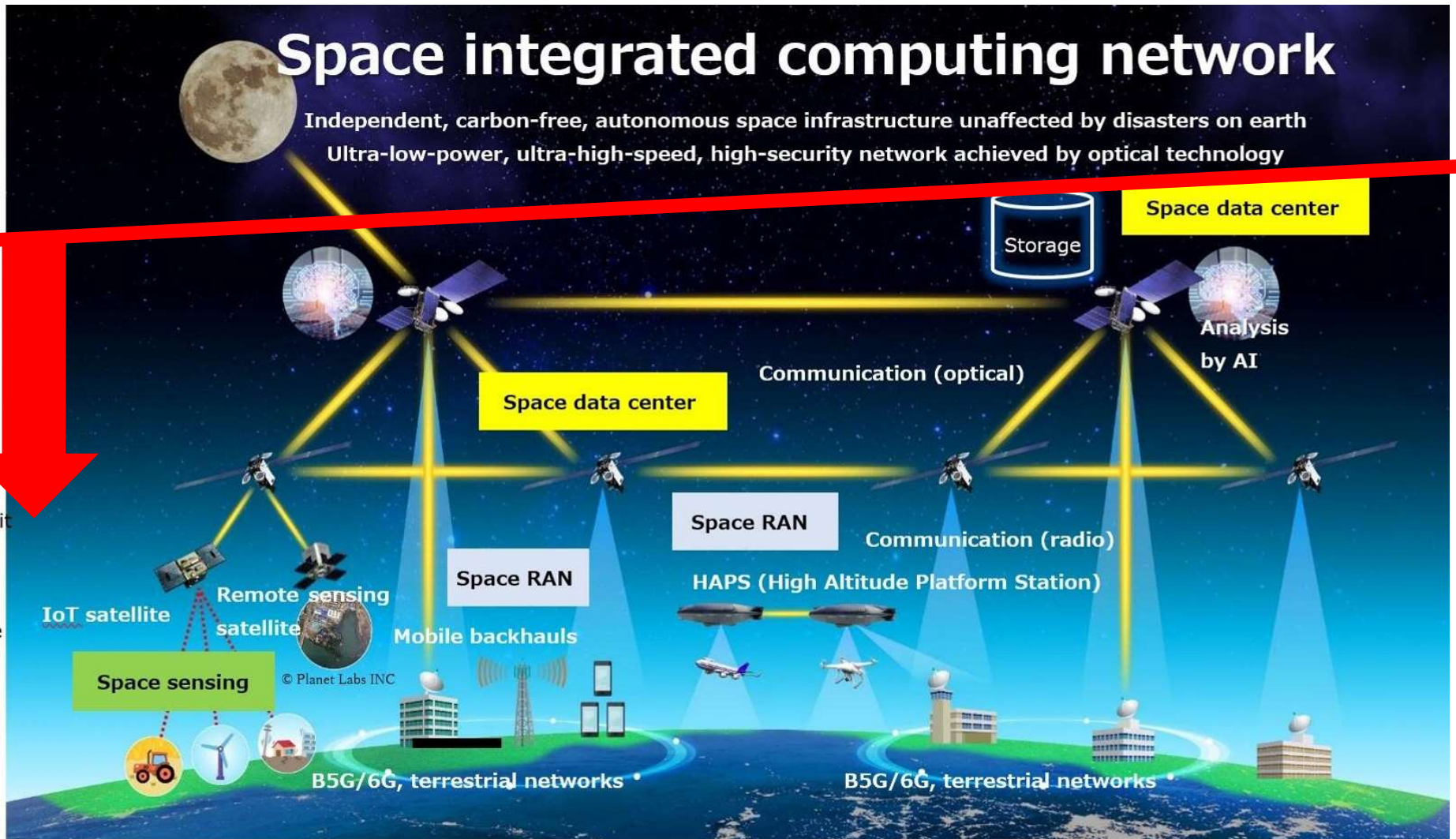
Geostationary orbit

Low Earth Orbit  
~1,000 km

Atmosphere  
20-50 km

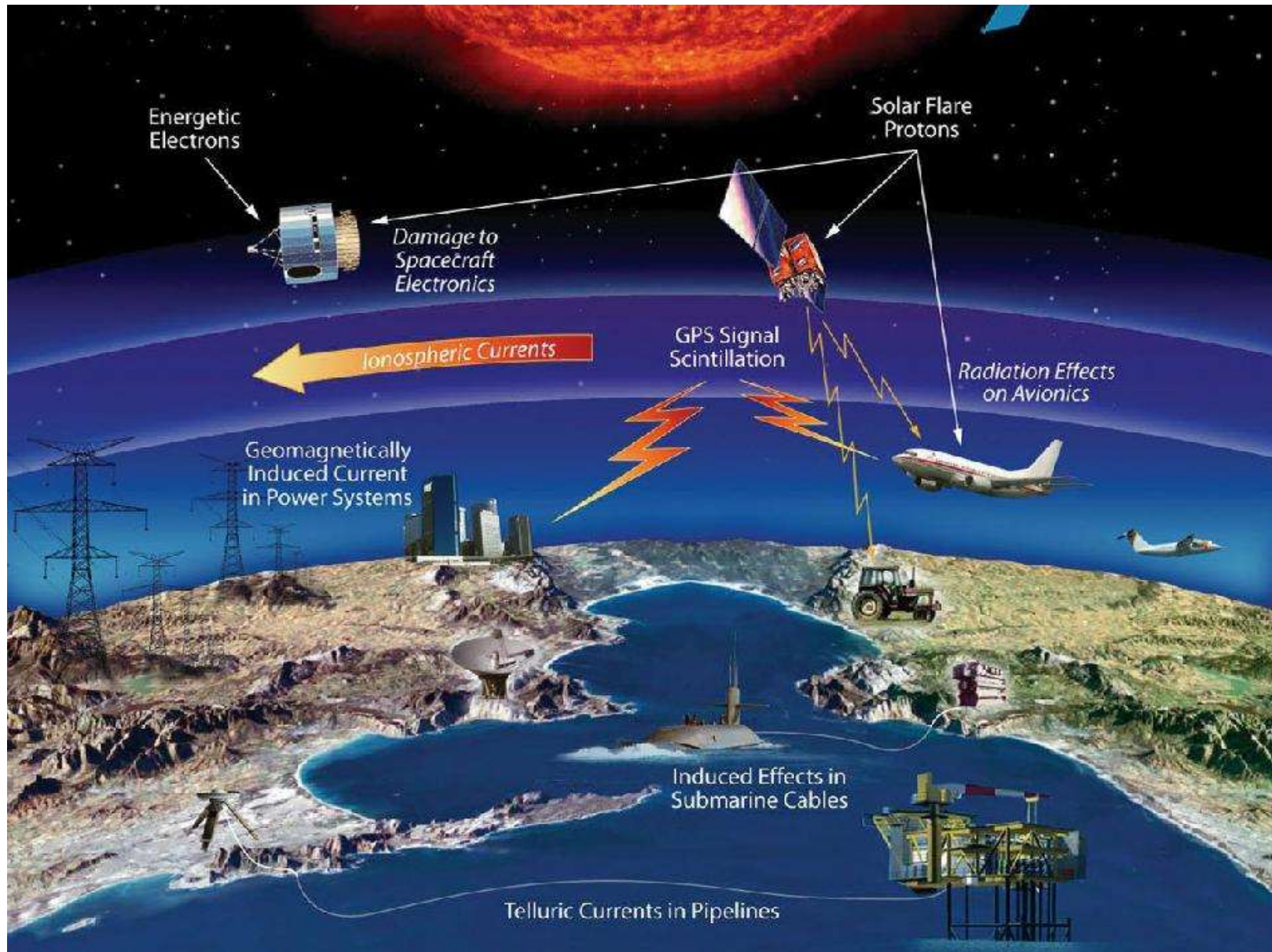
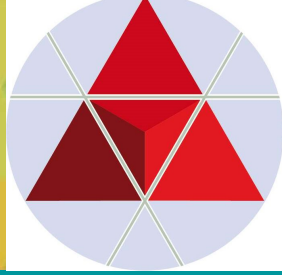
↓

Terrestrial





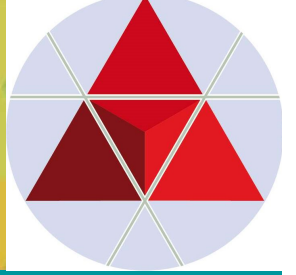
# Terrestrial & Space Infrastructure (SUPPLY CHAIN NETWORK)





# Overview 1: statistics (2023)

## Space-Objects & Debris (according to ESA)



### Space objects and debris by the numbers: (+ scrap metal)

Number of **rocket launches** since the start of the space age in 1957:

**About 6500 (excluding failures)**

Number of **satellites** these rocket launches have placed into Earth orbit:

**About 16990**

Number of **satellites still in space:**

**About 11500**

Number of **satellites still functioning:**

**About 9000**

Number of **debris objects regularly tracked by Space Surveillance Networks** and maintained in their catalogue:

**About 35150**

Estimated number of break-ups, explosions, collisions, or anomalous events resulting in fragmentation

**More than 640**

Total mass of all space objects in Earth orbit

**More than 11500 tonnes**

Not all objects are tracked and catalogued

**The number of debris objects estimated based on statistical models to be in orbit (Not all objects are tracked and catalogued):**

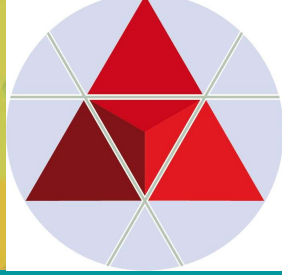
**36500 space debris objects greater than 10 cm**

**1000000 space debris objects from greater than 1 cm to 10 cm**

**130 million space debris objects from greater than 1 mm to 1 cm**

# Overview 2: statistics (2023)

## Space-Objects & Debris (according to ESA)



### Wer ist für den Weltraumschrott verantwortlich?

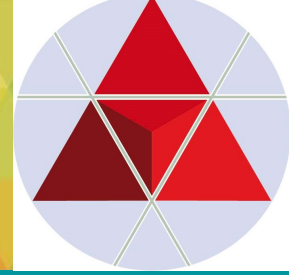
Anzahl verbrauchter Raketenteile/Trümmer aus ausgewählten Herkunftsländern/Organisationen



Quellen: ESA, NASA, OECD, Orbital Debris Quarterly News



# SUPPLY CHAIN RESILIENCE: Space infrastructure and attack vectors



## Segmente von Weltraum-Infrastruktur

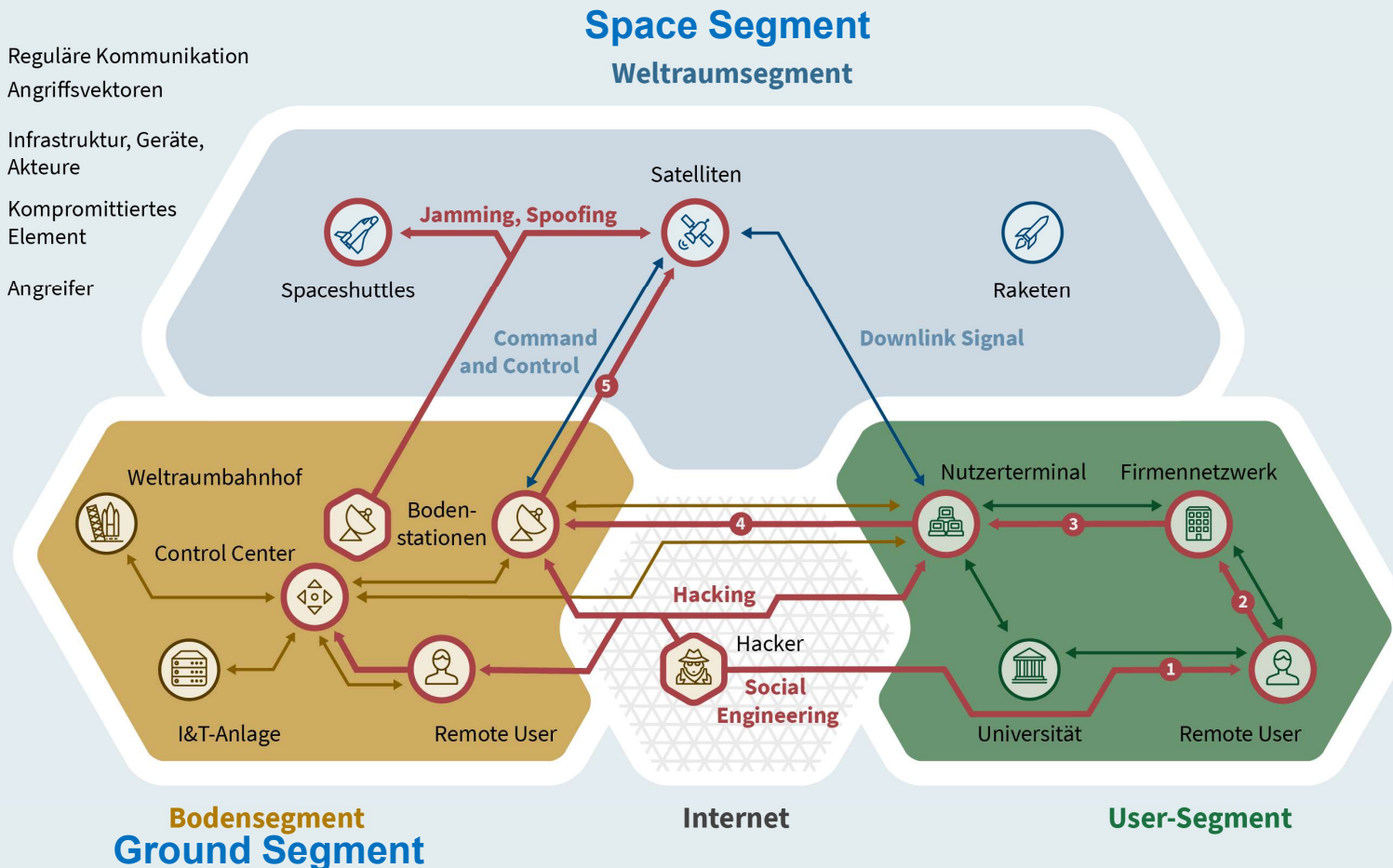
→ Reguläre Kommunikation

→ Angriffsvektoren

○ Infrastruktur, Geräte, Akteure

⊙ Kompromittiertes Element

⊙ Angreifer



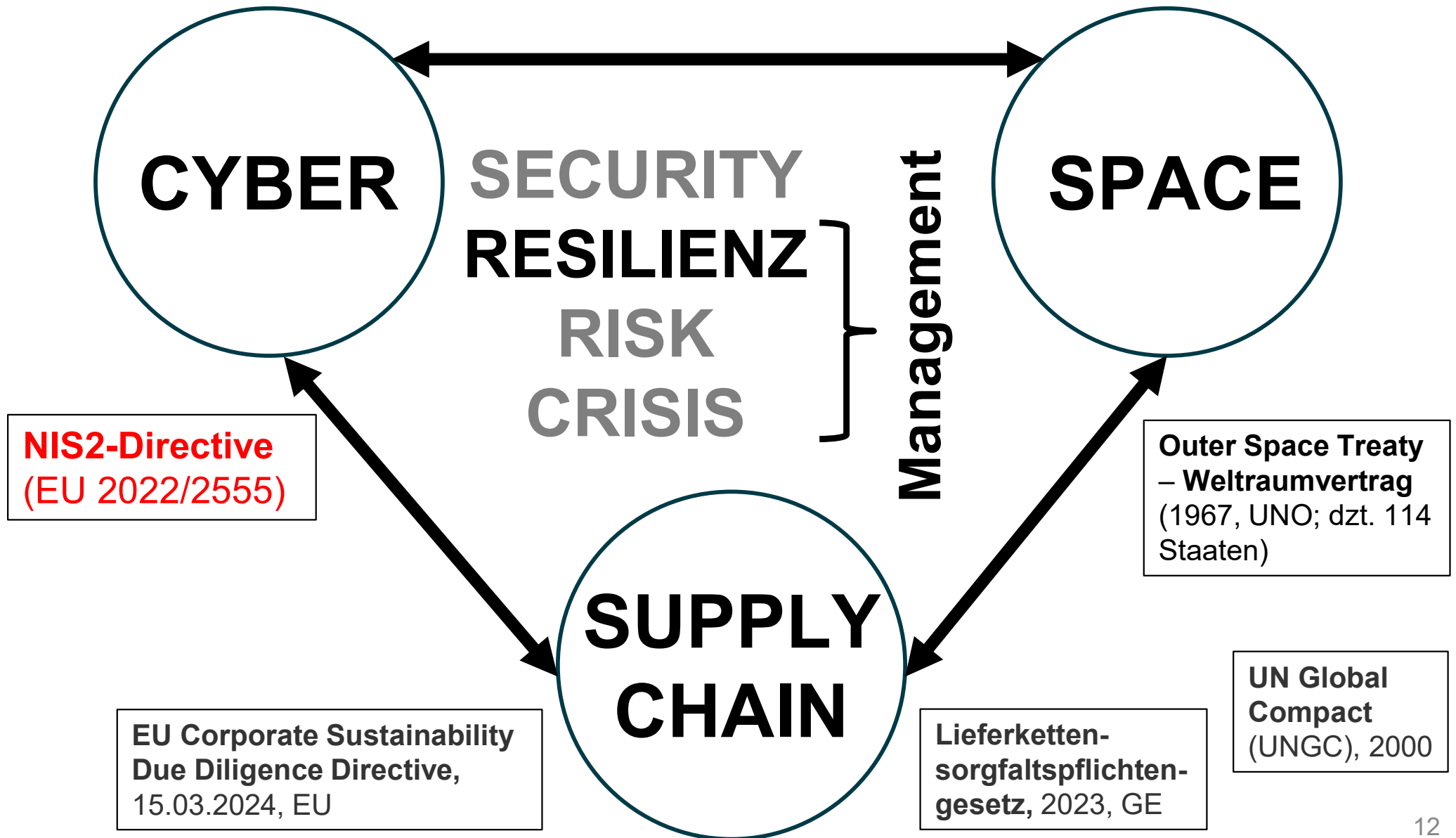
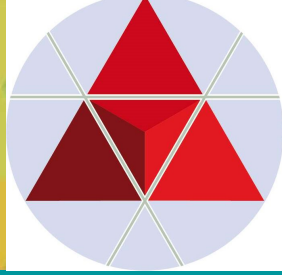
Diese Grafik ist in der Farbdarstellung am besten lesbar.

Quelle: [https://en.wikipedia.org/wiki/Ground\\_segment#/media/File:Ground\\_segment.png](https://en.wikipedia.org/wiki/Ground_segment#/media/File:Ground_segment.png)

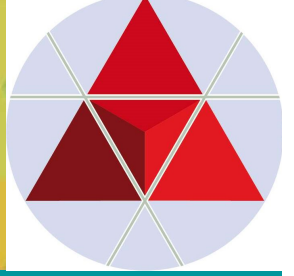
© 2023 Stiftung Wissenschaft und Politik (SWP)

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






# SUPPLY CHAIN RESILIENCE



# Supply Chain Risks & Losses:



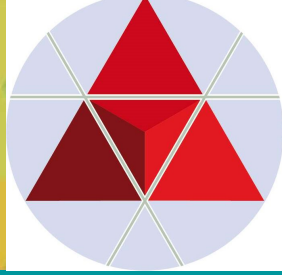
In framing financial discussions about losses due to supply chain risk, it is critical to analyze the operational impact of a disruption and the associated financial impact. Areas to look at include:

-  **1. Production stoppage or slowdown:** *Direct losses occur when production lines are forced to idle due to key components or inputs being unavailable. The daily cost of a halted production line is the most obvious cost but there may also be other related costs.*
-  **2. Higher freight costs:** *Inputs or even factory equipment can be flown in to reduce downtime, but this comes at a cost.*
-  **3. Lost sales:** *Extended stoppages where market demand remains can result in lost sales.*
-  **4. Loss of market share:** *For some industries lost sales can translate into lost market share where a competitor's product was found to be as good or better.*
-  **5. Reputation:** *Reputational risk is hard to measure but important as customer expectations of service and environmental stewardship grow. Even where the cause of a disruption is unavoidable, companies will still be expected to have done certain things to prepare for and respond to disruptions. Those that excel in this will find reputational upside by being the last to close and first to open.*

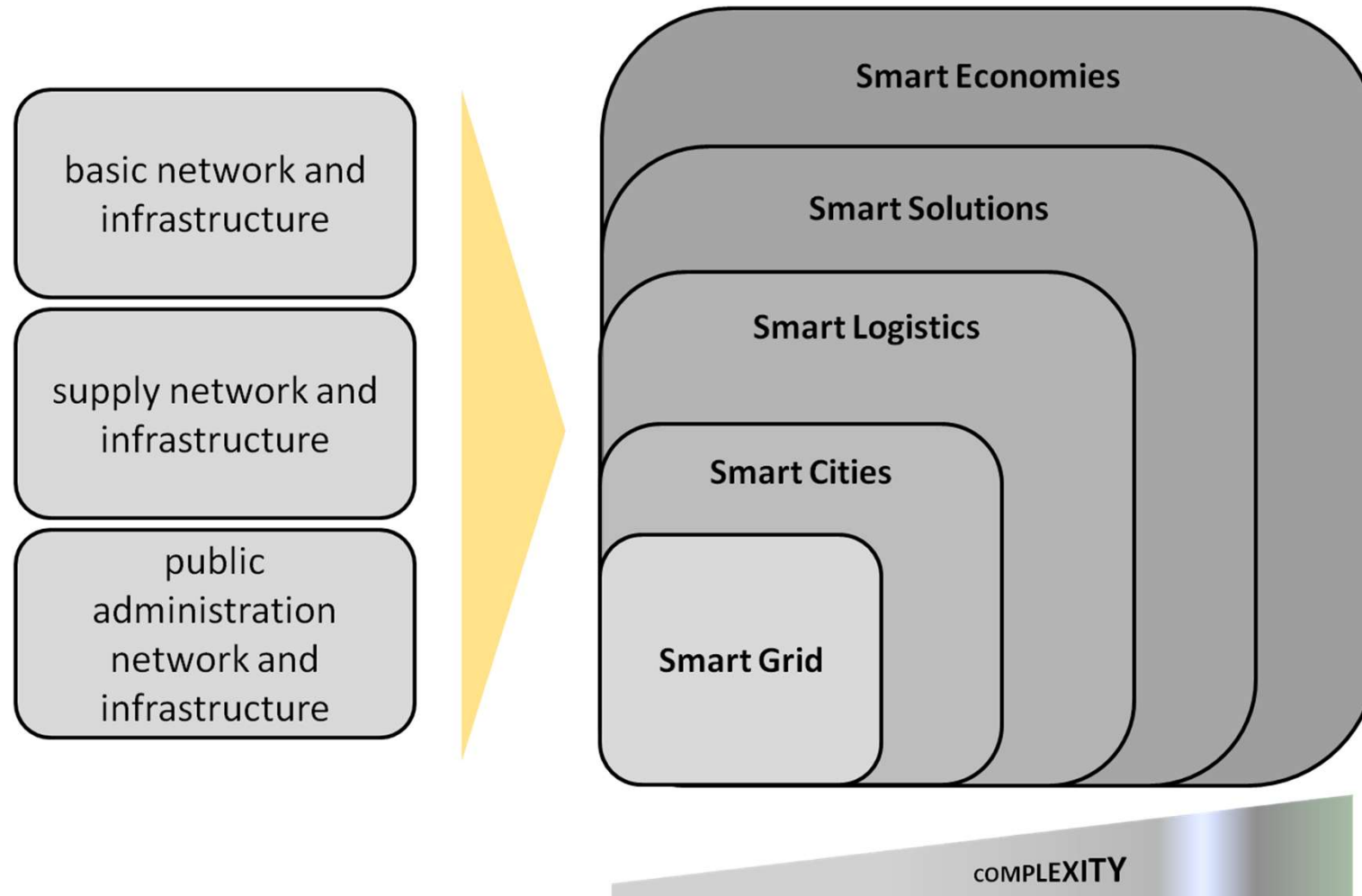
Every organization is on a learning curve for finding the right agility/redundancy balance for every link in their supply chain. Those who find the solution first will emerge as industry leaders.

# Supply Chain Risk- & Value Management

- *Supply Chain Resilience - Requirements*



## Global Supply Chain Networks






# Principles of supply chain security







How to gain and maintain control of your supply chain

The principles are divided into four stages representing the process of securing your supply chain. To find out more visit:  
[www.ncsc.gov.uk/guidance/supply-chain-security](http://www.ncsc.gov.uk/guidance/supply-chain-security)

## I. Understand the risks

-  Understand what needs to be protected and why
-  Know who your suppliers are and build an understanding of what their security looks like
-  Understand the security risk posed by your supply chain



## II. Establish control

-  Communicate your view of security needs to your suppliers
-  Set and communicate minimum security requirements for your suppliers
-  Build security considerations into your contracting processes and require that your suppliers do the same
-  Meet your own security responsibilities as a supplier and consumer
-  Raise awareness of security within your supply chain
-  Provide support for security incidents

## III. Check your arrangements

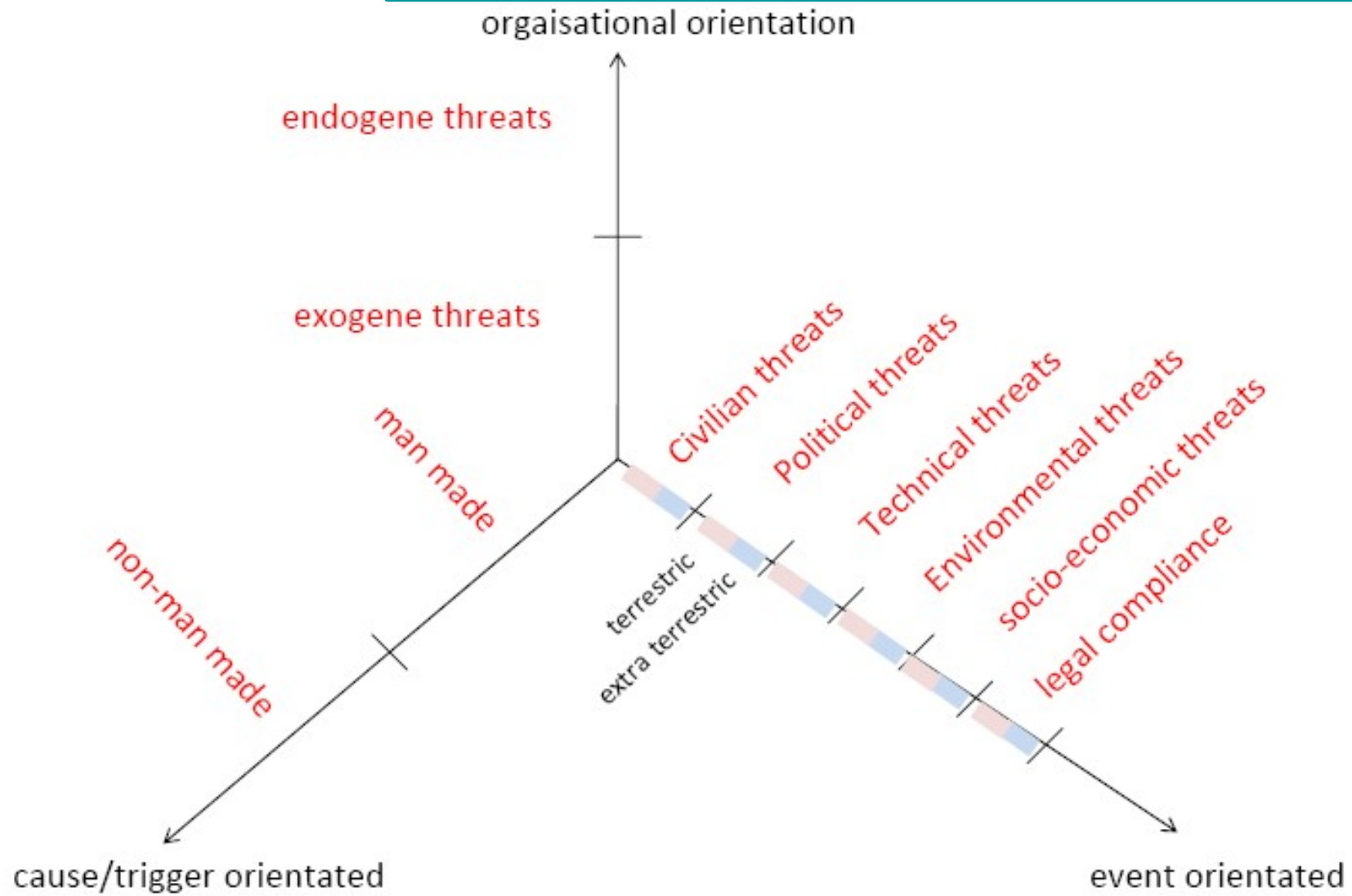
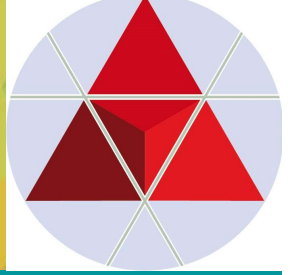
-  Build assurance activities into your approach to managing your supply chain

## IV. Continuous improvement

-  Encourage the continuous improvement of security within your supply chain
-  Build trust with suppliers

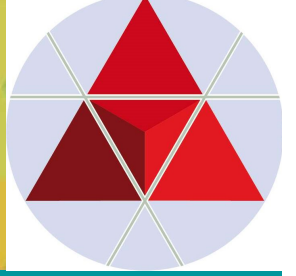


# ● Meta Model of a Event/Risk Analysis





# Kontakte



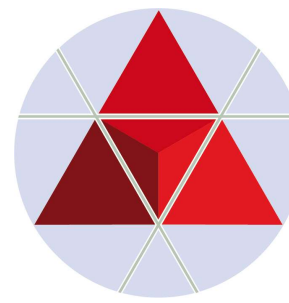
## Johannes L. GOELLNER

*Chairman of the Board*

**Zentrum für Risiko- und Krisenmanagement, Vienna  
[Center for Risik- and Crises Management, Vienna]**

[www.zfrk.org](http://www.zfrk.org)

*E-mail: [johannes.goellner@zfrk.org](mailto:johannes.goellner@zfrk.org)*



Zentrum für  
Risiko- & Krisenmanagement

**Thank you for your attention.**

excellent.  
connected.  
individual.