IKT-Sicherheitskonferenz 2024
Wien/Österreich, 17.09.2024-18.09.2024
Vortragszeit: 17.09.2024, 11:45-12:05 Uhr,
Raum: SCHUBERT 4

Zentrum für
Risiko- & Krisenmanagement

Die ökonomische , infrastrukturelle und finanzwirtschaftliche Bedeutung des Weltraumes

Dipl.-Ing. Johannes GÖLLNER, MSc (ZRK, Wien)

- *(Vortragsbasis: Johannes Göllner & Ralf A. Huber (iRd RMC 2024, 13.05.2024, Hamburg)*

excellent.
connected.
individual.

VSSC 2024
VIENNA SPACE SECURITY CONFERENCE

AGENDA:

1. **PRESSEMELDUNGEN**
2. **INVESTMENTS-***Kurzdarstellung*
3. **SUPPLY CHAIN RESILIENCE**
4. **REGULATORIK**

PRESSE-MELDUNGEN

PRESSEMELDUNGEN: SUPPLY CHAIN & CYBER

Zurück

Dienstag, 09.04.2024

Seite 2 von 28

2 RESILIENZ contentway

RESILIENZ

contentway

AUSGABE #151

Campaign Manager:
Manh Nam „Manni" Nguyen

Geschäftsführung:
Nicole Bitkin

Head of Content & Media Production:
Aileen Reese

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

Text:
Silja 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 Schadsoftware-Varianten bekannt.

Resilienz ist mehr als Krisenmanagement

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

EINLEITUNG

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

Foto: Presse

Dienstag 9. Apr.

37 %

rück

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 auditierbar 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 Cybersicher-

irück

Dienstag, 09.04.2024

Seite 6 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

ck

Dienstag, 09.04.2024

Seite 17 von 28

Möhrle Happ Luther – Partner Content

contentway.de RESILIENZ 17

NIS2: Europas Schutzschild gegen Cyberkriminalität

Ab Oktober 2024 müssen alle Unternehmen in Europa mit mindestens 50 Mitarbeitern und zehn Millionen 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.

anche Länder finanzieren

view über mögliche Angriffsszenarien und Unterstützung der IT.

Herr Köhne, was sind denn 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. Besorgniserregend 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

PRESSEMELDUNGEN: SPACE

Handelsblatt

Raumfahrt

Geschäft mit dem Weltraum wird zur 1,25-Billionen-Euro-Chance

Autobranche, Konsum oder Energie: Raumfahrttechnologie eröffnet laut einer neuen Studie riesige Märkte für die deutsche Industrie – „vergleichbar mit China".

Thomas Jahn
17.10.2023 - 18:26 Uhr

ETH zürich

News & Veranstaltungen | Die ETH Zürich | Studium | Doktorat | Forschung | Wirtschaft & Wissenstransfer | Campus

Startseite › News & Veranstaltungen › ... › 2023 › Mai › Ehemaliger NASA-Forschungschef kommt an die ETH Zürich

FORSCHUNG · ERDWISSENSCHAFTEN

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 von ETH Zürich Space. Mit dieser Initiative soll die Weltraumforschung und -lehre an der ETH ausgebaut und die Zusammenarbeit mit der Raumfahrt-Industrie gestärkt werden.

STEIERMARK LEBEN SPORT KLEINE ZEITUNG

Ausflug ins All für Österreichs ersten Weltraumtouristen

PORTRÄT. **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

WELTRAUMSCHROT

US-Behörde verhängt Strafe gegen Satellitenbetreiber

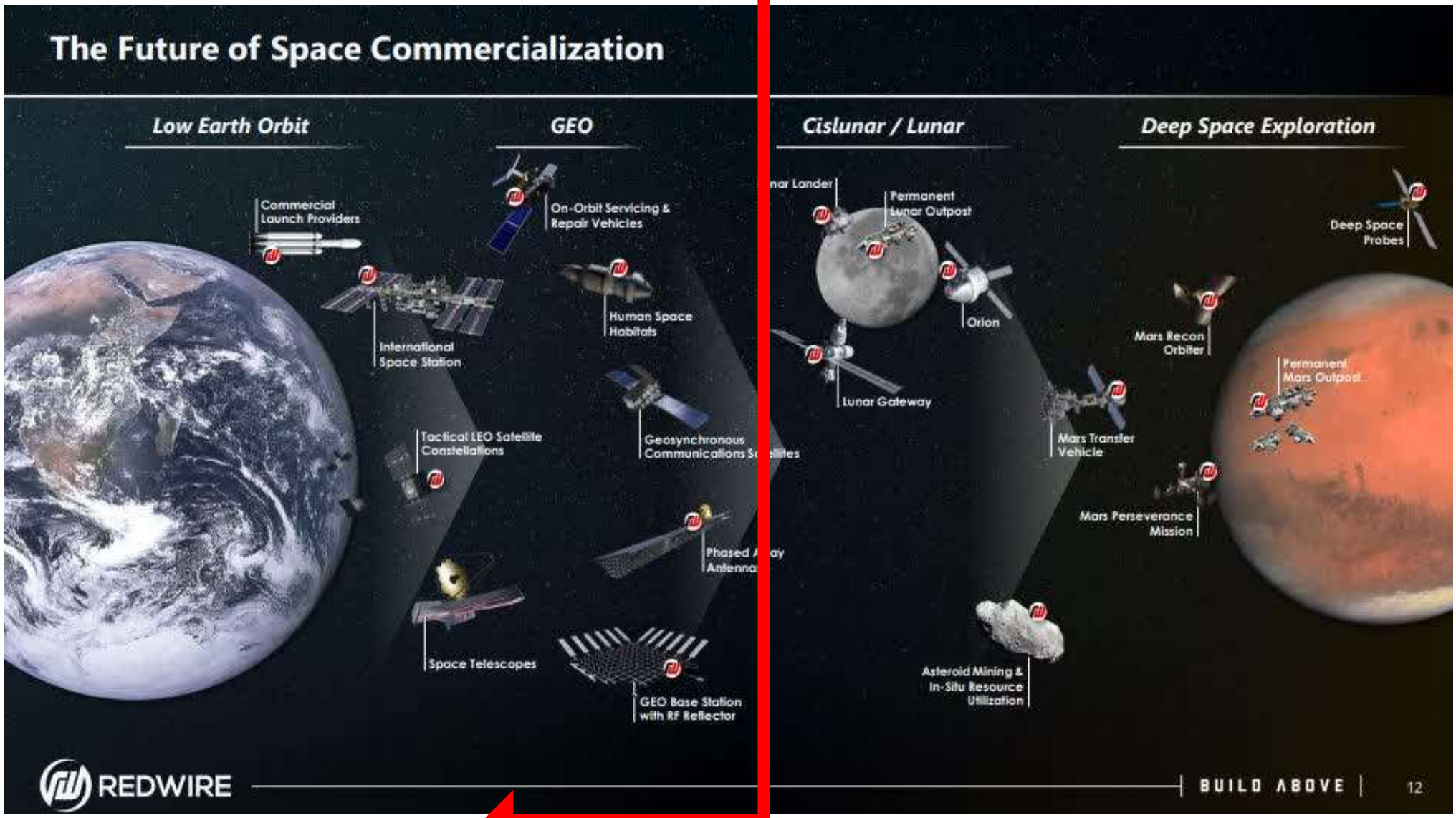
Ein stillgelegter Satellit muss dorthin gebracht werden, wo er keine Gefahr darstellt. Ein Betreiber muss Strafe zahlen, weil er dem nicht nachgekommen ist.

in Pocket speichern | merken

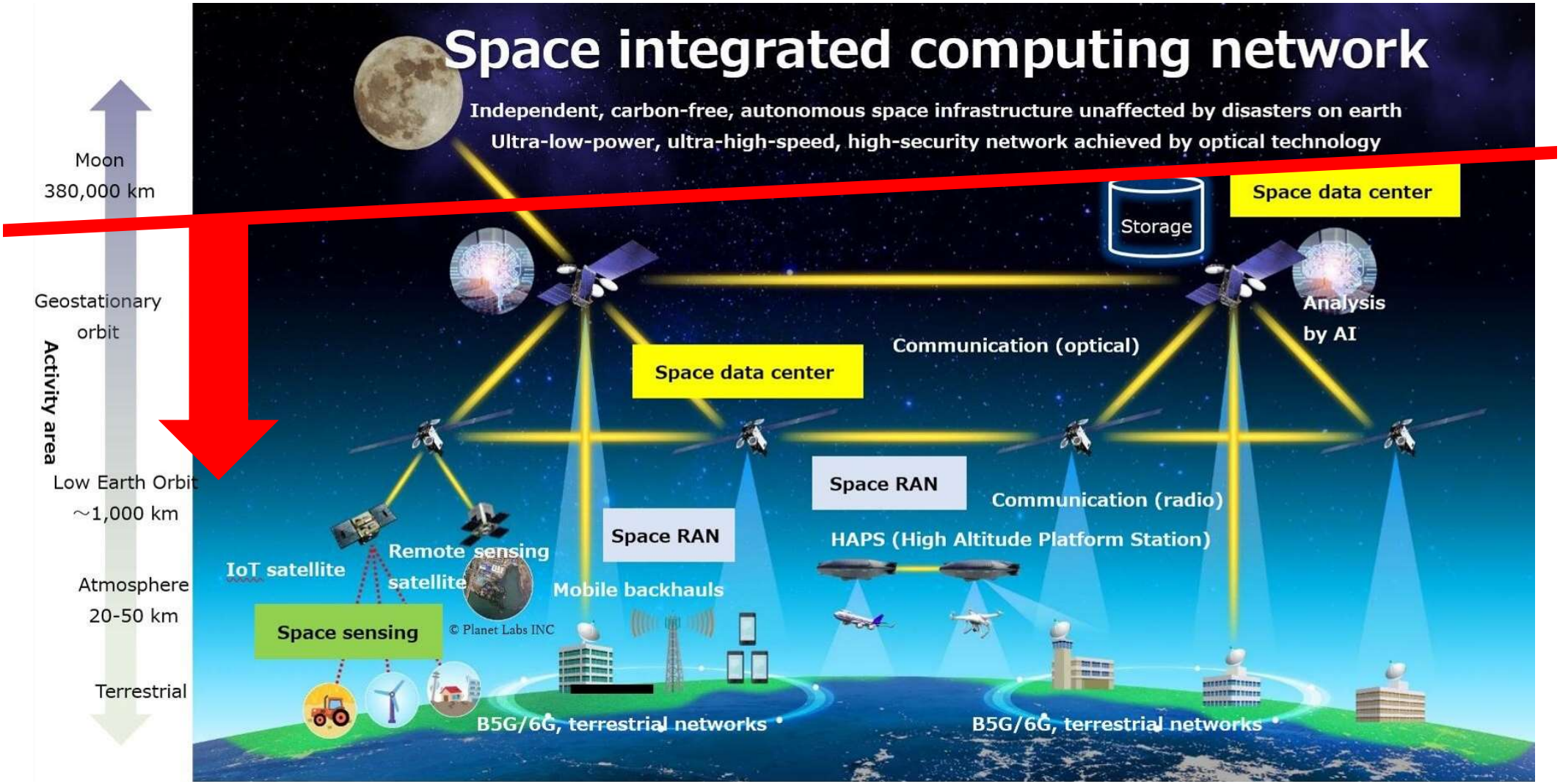
5. Oktober 2023, 11:31 Uhr, Werner Pluta

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

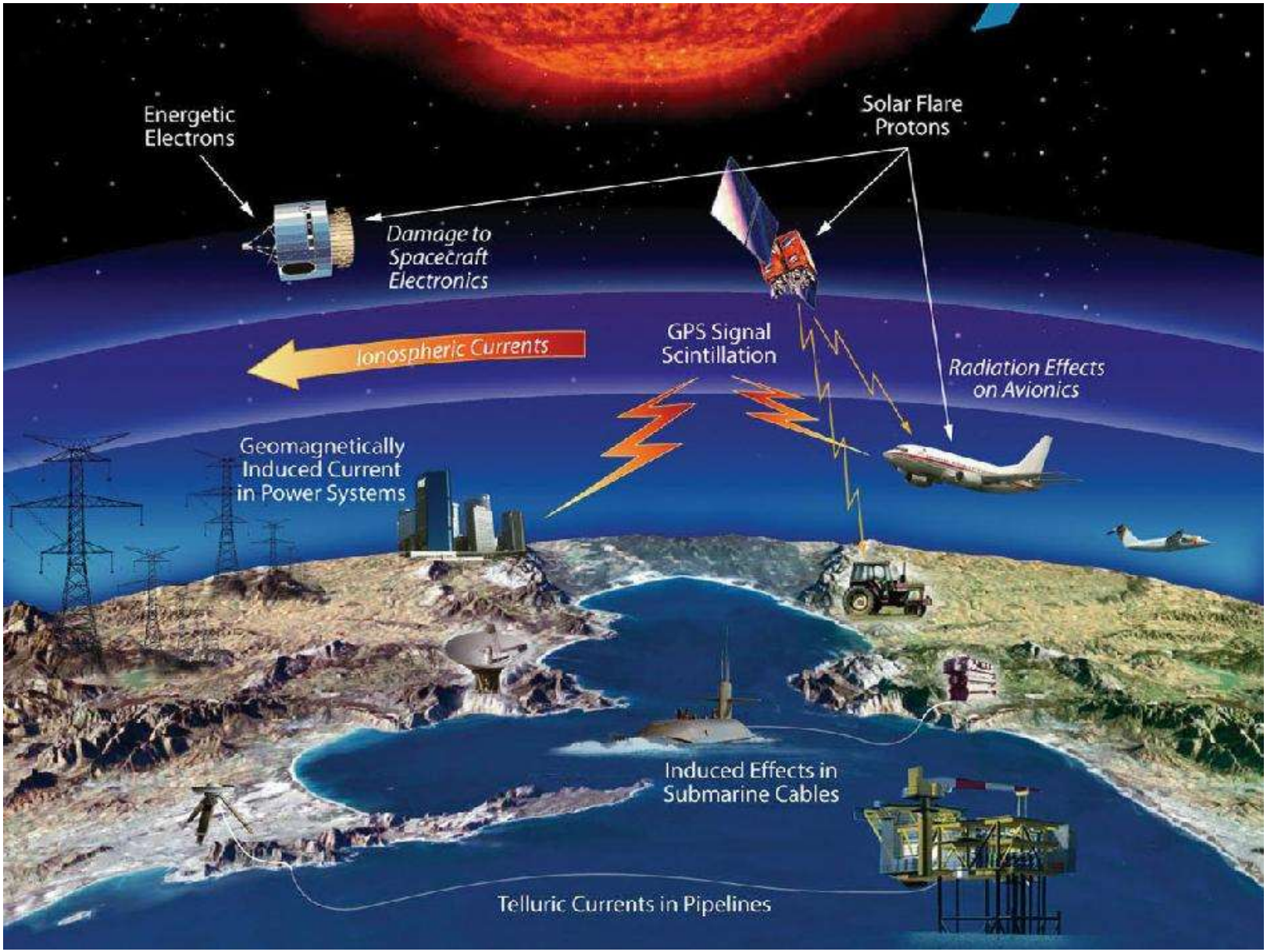
Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



Überblick 1: STATISTIKEN (2023)
WELTRAUM-Objekte (gem. ESA)

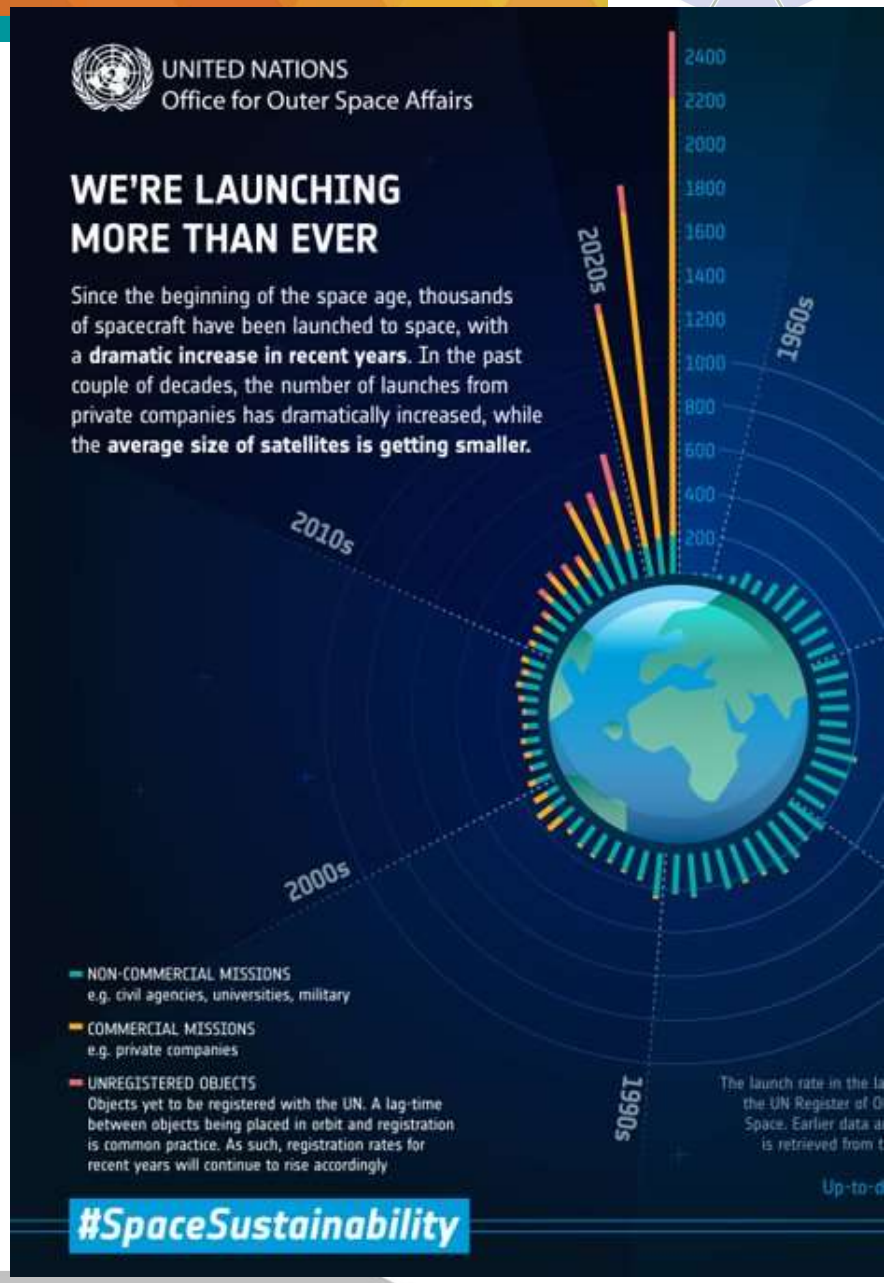
Space objects and debris by the numbers:

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
1.000.000 space debris objects from greater than 1 cm to 10 cm
130 million space debris objects from greater than 1 mm to 1 cm

Souce: Space debris by numbers, ESA, Last update: 06.December 2023, Space Environment Statistics · Space Debris User Portal (esa.int)

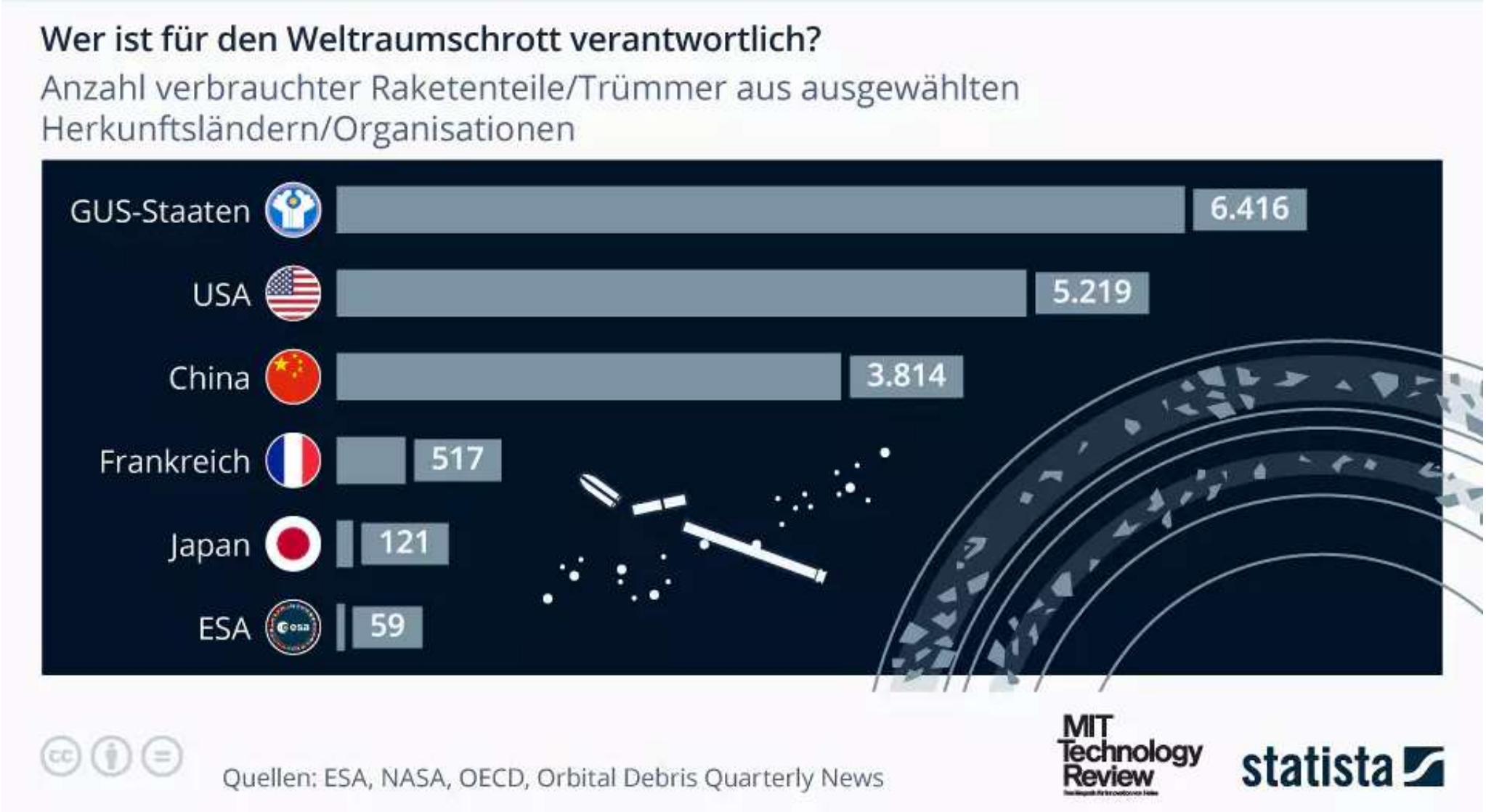
Verwundbarkeiten: Mannigfaltige verknüpfte Angriffsflächen rund um Kommunikation

- **“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"**



Source: Alexander Siedschlag, ZRK & ERAU, Vortrag IKT SIKON 2023

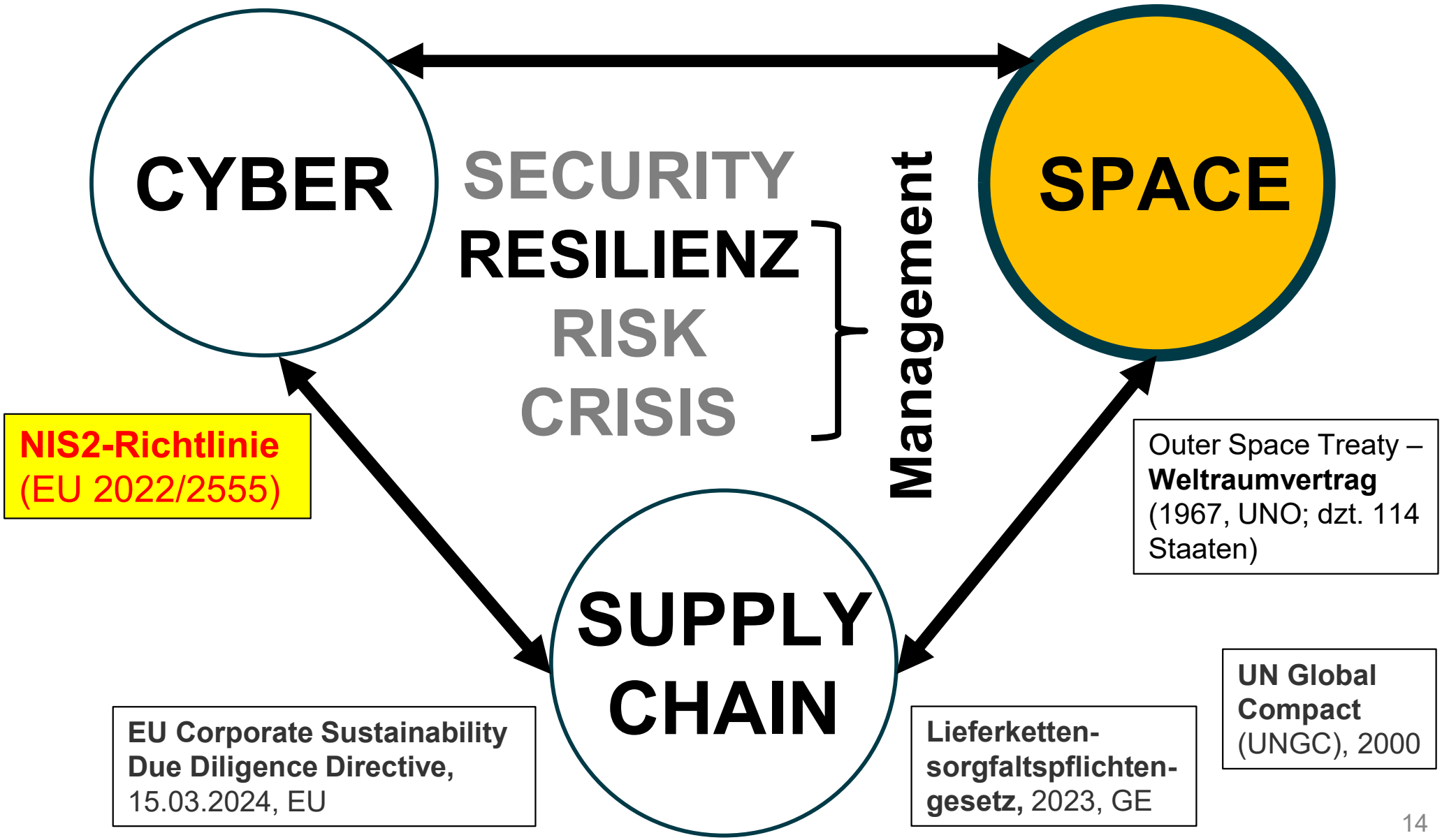
Überblick 3: STATISTIKEN (2023)
WELTRAUM-Objekte (gem. statista)



INVESTMENTS

SUPPLY CHAIN RESILIENCE

SUPPLY CHAIN RESILIENZ



Überblick: STATISTIKEN (2023)
- weltweit % (+AT; +GE; +CH;)

The 10 largest global business risks in 2023

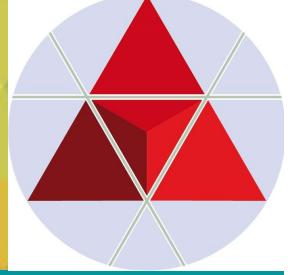
1. **Cyber Events: 34**% (AT: **40**%; GE: **40**%; CH: **57**%)
2. **Supply Chain Interruption-Betriebsunterbrechnung**: **34%** (AT: **32**%; GE: **46**%; CH: **41**%))
3. Makroökonomische Veränderungen: **25**% (AT: **24**%; GE: **17**%; CH: **14**%))
4. Energiekrise: **22%** (AT: **38**%; GE: **32**%; 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**%))

Zusammenfassung: Johannes GÖLLNER, Vortrag IKT SIKON 2023

Source: Allianz Global Corporate & Specialty in Allianz Risk Barometer 2023: Die 10 größten Geschäftsrisiken 2023, Weltweit

Description of (Global) Supply Chain Networks:



II. Supply Networks

e.g.:

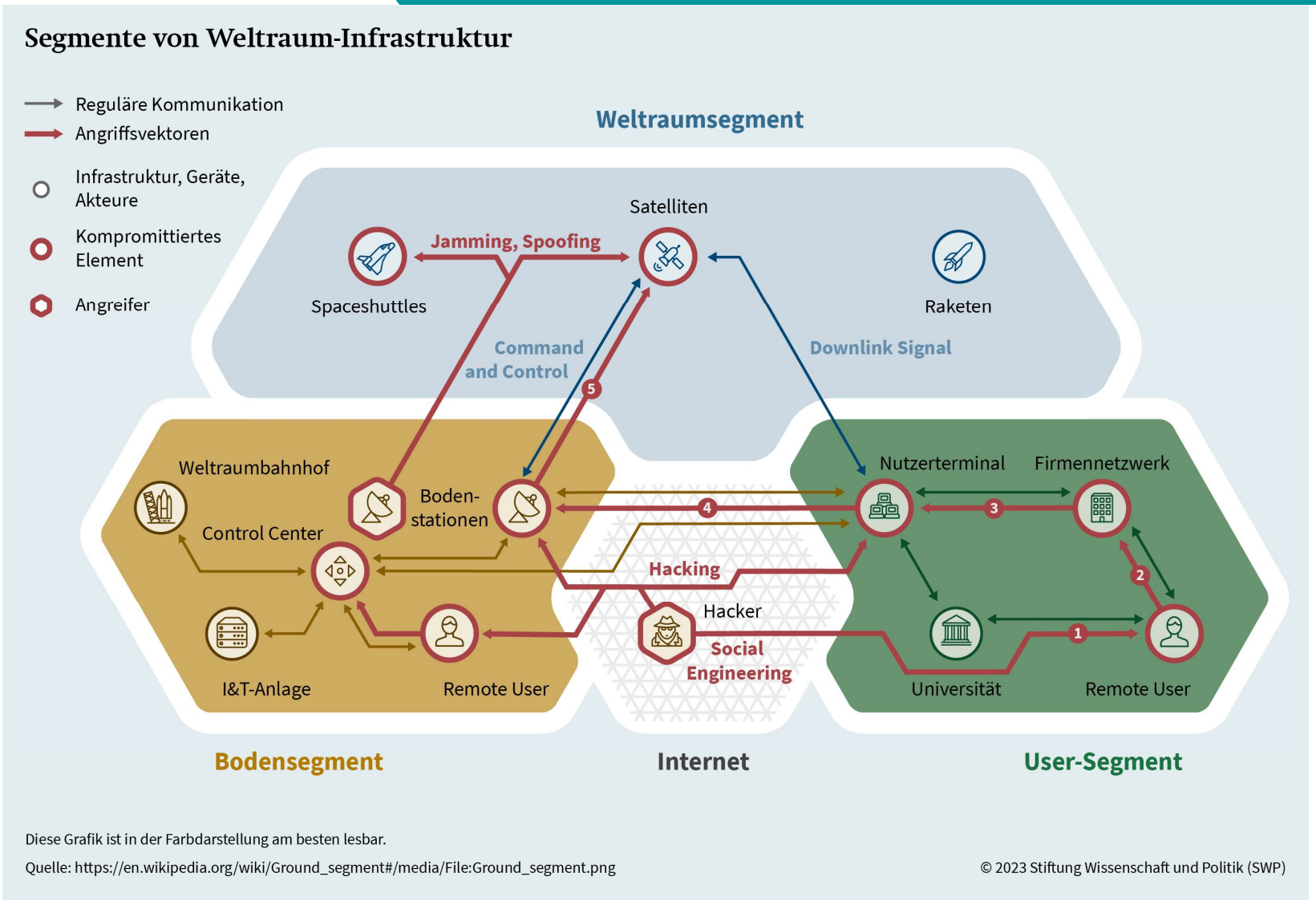
- Financial Networks
- Resource/Raw Material Networks (criticality)
- Food Supply Network
- Water Supply Network
- etc.

I. Basic Networks

- Transport/Traffic-Networks
  - (Air, Road, Railway, Waterways)
- ICT-Networks (+/-: Smart Grids)
- Energy Networks (+/-: Smart Grids)

III. Governmental & Public-/Administration Networks

SUPPLY CHAIN RESILIENZ: Weltraum-Infrastruktur und Angriffsvektoren



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

Source: Alexander Siedschlag, ZRK & ERAU, Vortrag IKT SIKON 2023

Supply Chain Risks & Losses:

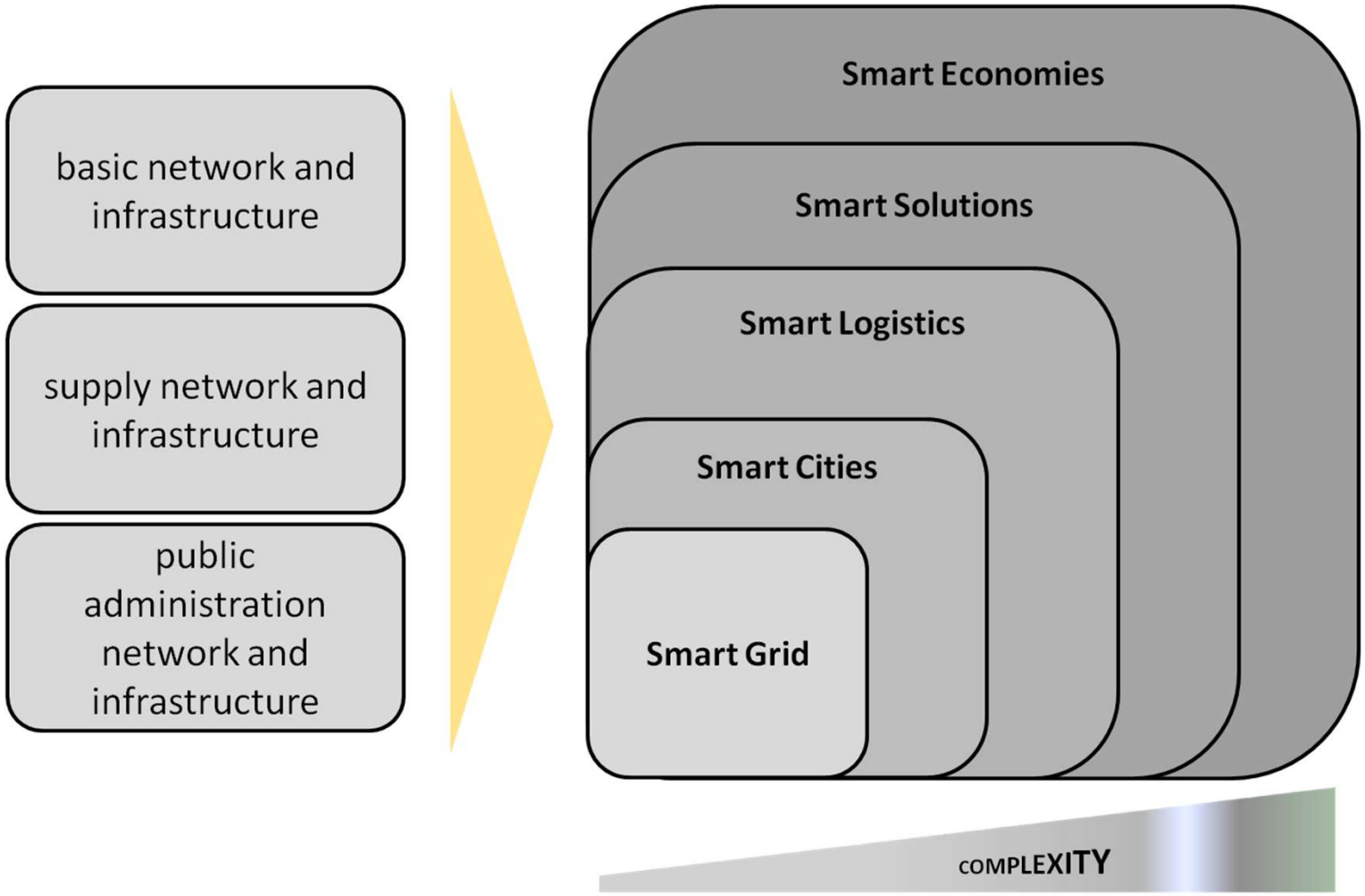
In framing financial discussions about losses due to supply chain risk, it is critical to analyze the operational impact of a disruption and the associated financial impact. Areas to look at include:

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.

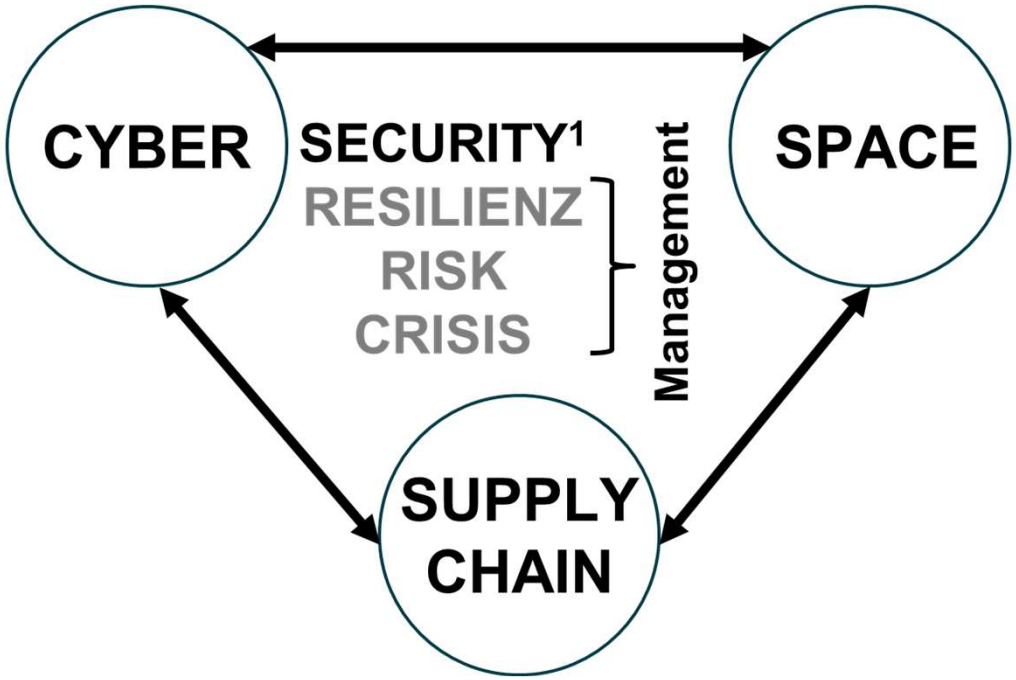
Source: Risky Business:What Supply Chain Disruptions Really Cost, Everstream Analytics, 02.02.2022, www.everstream.ai

Global Supply Chain Networks



REGULATORIK

SECURITYZATION-CONCEPT



[2] „Weltraumpolitik ist Sicherheitspolitik-erst danach bedeutet der Weltraum Technik oder Recht. Für DE hingegen existiert derzeit kein weltraumpolitischer –sicherheitspolitischer und völkerrechtlicher –Rahmen für die staatliche Sicherheitsvorsorge. Gleichwohl stellt das Weißbuch von 2016 inzwischen hierzu fest, dass **DE´s sicherheitspolitischer Horizont global ist und dieser ausdrücklich auch den Cyber-, Informations- und Weltraum umfasst.** *(siehe BMVg (Hrsg.), Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr, Berlin 2016, S.56.)*

[1]Securityzation-Concept:

- **societal security,**
- **political security[2],**
- **economical security,**
- **environmental security,**
- **public security,**
- **cyber security,**
- **space security.**

in Anlehnung an das “Securityzation Concept-New framework of analysis” von BUZAN/WEAVER/WILDE (2001)

The NIS 2 Directive

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022

The measures shall be based on an "all-hazards approach" that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include "at least" the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

CYBER- SPACE & SUPPLY CHAIN SECURITY: NIS 2-Richtlinie (EU 2022/2555)

Wesentliche Einrichtungen (Anhang I)	Wichtige Einrichtungen (Anhang II)
Energie (Elektrizität, Fernwärme/kälte, Öl, Gas, Wasserstoff)	Post- und Kurierdienste
Verkehr (NIS 1: Luft, Wasser, Schiene, Straße)	Forschung
Bankwesen	Chemie (Herstellung & Handel)
Finanzmarktaufsichtinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU- Referenz-laboratorien, Forschung und Herstellung pharmazeutischer und medizinischer Produkte & Geräte)	Verarbeitendes & Herstellendes Gewerbe: (Medizinprodukte; Datenverarbeitungs- elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste, Suchmaschienen, Online-Marktplätze, Plattformen für Dienste sozialer Netzwerke
Abwasser	
Digitale Infrastruktur (IXP, DNS, TLD, Cloud Computing, Rechenzentren, Inhaltszustellnetzen, Vertrauensdiensteanbieter, und öffentliche elektronische Kommunikationsnetze)	Abfallbewirtschaftung *(Anmerkung GÖLLNER: „Kreislaufwirtschaft:Circular Economy integriert JA/NEIN ?!)“*
IKT-Service Management	
Öffentliche Verwaltung	
Weltraum (SPACE)	

Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

National Cyber Security Centre
a part of GCHQ

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

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

CPNI
Centre for the Protection of National Infrastructure

https://www.ncsc.gov.uk/files/supply_chain_ncsc_cpni_2.pdf

www.ncsc.gov.uk @ncsc

Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

Andere relevante Regelwerke wie Standards, Leitfäden und Publikationen: (*auszugsweise*)

Risikomanagement:

- ***ISO 31000 & EN 31010*** *(grundsätzlich relevant!)*

Supply Chain Security Management:

- ***ISO 28000*** *(Specification for security management systems for the supply chain), First edition: 2007-09-15; aktueller Stand: ISO 28000:2022; Revision in Vorbereitung.*
- ***ISO 28001*** *(Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans Requirements and Guidance), First edition 2007-10-15;*
- ***ISO 20858*** *(Ships and marine technology — Maritime port facility security assessments and security plan development), First edition 2007-10-15; aktueller Stand: ISO 28000:2012;*

Krisenmanagement: vs. BCM *(vgl. NIS 2)*

- ***ISO 22361*** *(Security and resilience — Crisis management — Guidelines), First edition 2021-11-05; aktueller Stand: ISO 22361:2022;*

KONSEQUENZ-MANAGEMENT

Anwendungsbereich:

- Anwendungsbereich durch „size cap rule“ vorgegeben (“cap-size rule” for the identification of regulated entities.)
- **NIS-2 gilt für alle öffentlichen oder privaten wesentliche und wichtige Einrichtungen** der in Anhang I und Anhang II genannten Art, die Ihre Dienstleistungen in der EU erbringen oder Ihre Tätigkeiten in der EU ausüben und die den Schwellenwert für mittlere Unternehmen iSd Empfehlung 2003/361/EG der EU-Kommission erreichen oder überschreiten.
- **Kleinst- und Kleinunternehmen nur in bestimmten Fällen betroffen von NIS-2.**

Schwellenwerte:

- **Großunternehmen:** Alle Unternehmen, die nicht KMU sind.
- **Mittleres Unternehmen:**
  - < 250 MA; höchstens EUR 50 Mio Jahresumsatz oder Jahresbilanzsumme: höchstens EUR 43 Mio
- **Kleinst- und Kleines Unternehmen:**
  - < 50 MA und dessen Jahresumsatz <= EUR 10 Mio ist.

Geldbußen (Art 34): (bei Verstoß gegen Art 21 & Art 23)

- **Wesentliche Einrichtungen:** max. EUR 10.000.000 Mio oder einem Höchstbetrag von mind. 2 % weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres **des Unternehmens, dem die wichtige Einrichtung angehört.**
- **Wichtige Einrichtungen:** max. EUR 7.000.000 Mio oder einem Höchstbetrag von mind. 1,4 % weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres **des Unternehmens, dem die wichtige Einrichtung angehört.**

Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

VSSC 2024
VIENNA SPACE SECURITY CONFERENCE

Zentrum für
Risiko- & Krisenmanagement

Thank you for your attention.

excellent.
connected.
individual.

DI Johannes GOELLNER

Vorstandsvorsitzender

Zentrum für Risiko- und Krisen Management (ZRK)

(Center of Risk and Crises Management-CRC)

A-1180 Vienna, Reisnerstrasse 5/20a, Austria

M: +[43]-650-2252991

email: johannes.goellner@zfrk.org

Zentrum für
Risiko- & Krisenmanagement