**IKT-Sicherheitskonferenz 2025**
Dornbirn, 25.06.2025-26.06.2025
Vortragszeit: 25.06.2025, 13:45-14:15 Uhr,
Raum: Halle 14 Side Stage

Zentrum für
Risiko- & Krisenmanagement

# Resilienz: Cyber-, Supply Chain und Space Security


- **DI Johannes GÖLLNER** (ZRK, Wien)
- **Ralf A. HUBER** (Staedtler SE, Nürnberg)


excellent.
connected.
individual.

# AGENDA:

1. PRESSEMELDUNGEN
2. SUPPLY CHAIN RESILIENCE
3. REGULATORIK
4. RMA-LEITFADEN:
   „SUPPLY CHAIN RESILIENCE MANAGEMENT“
5. FAZIT & AUSBLICK

# 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



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.**

Manche 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.

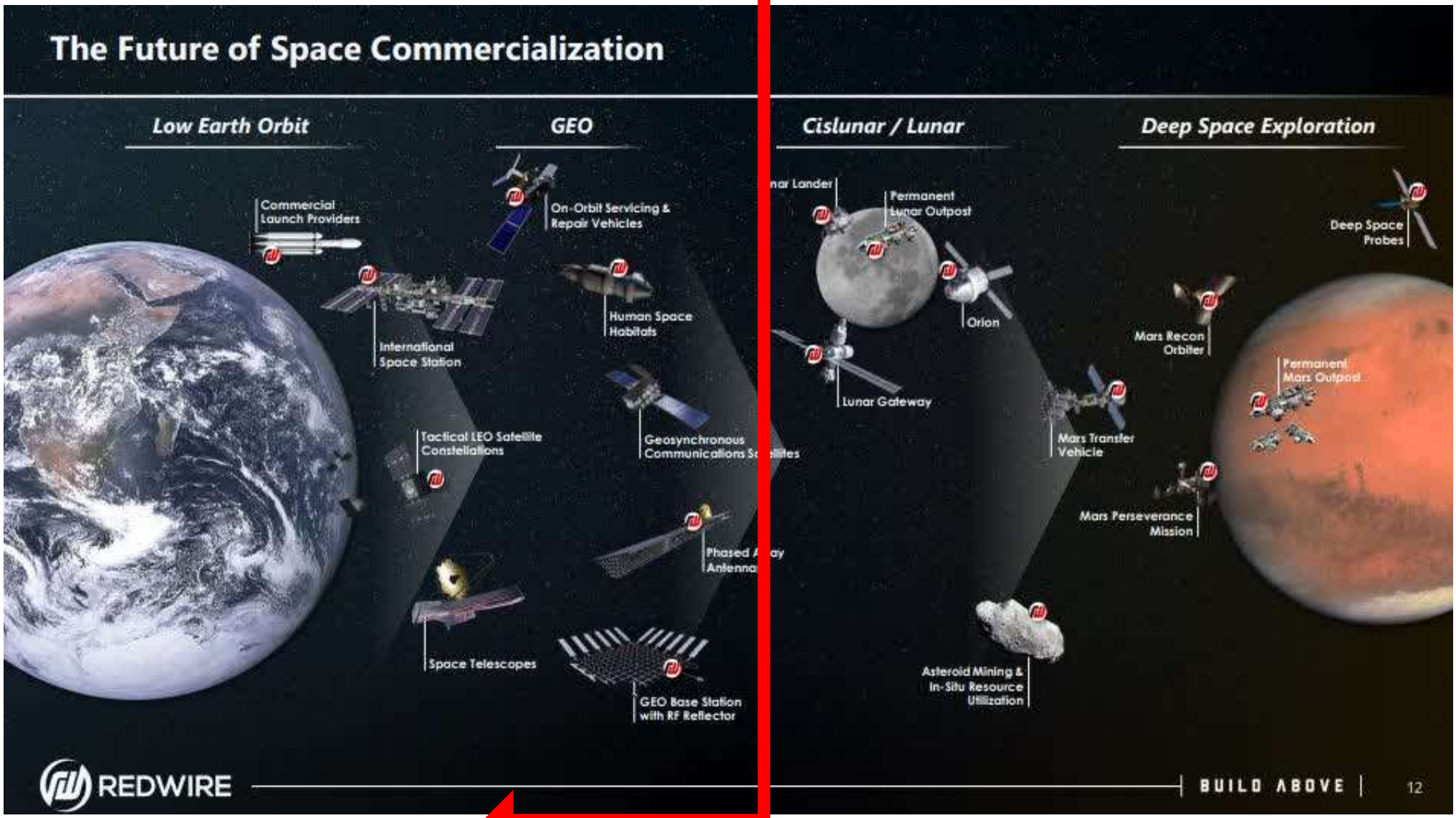
in Pocket speichern | merken

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

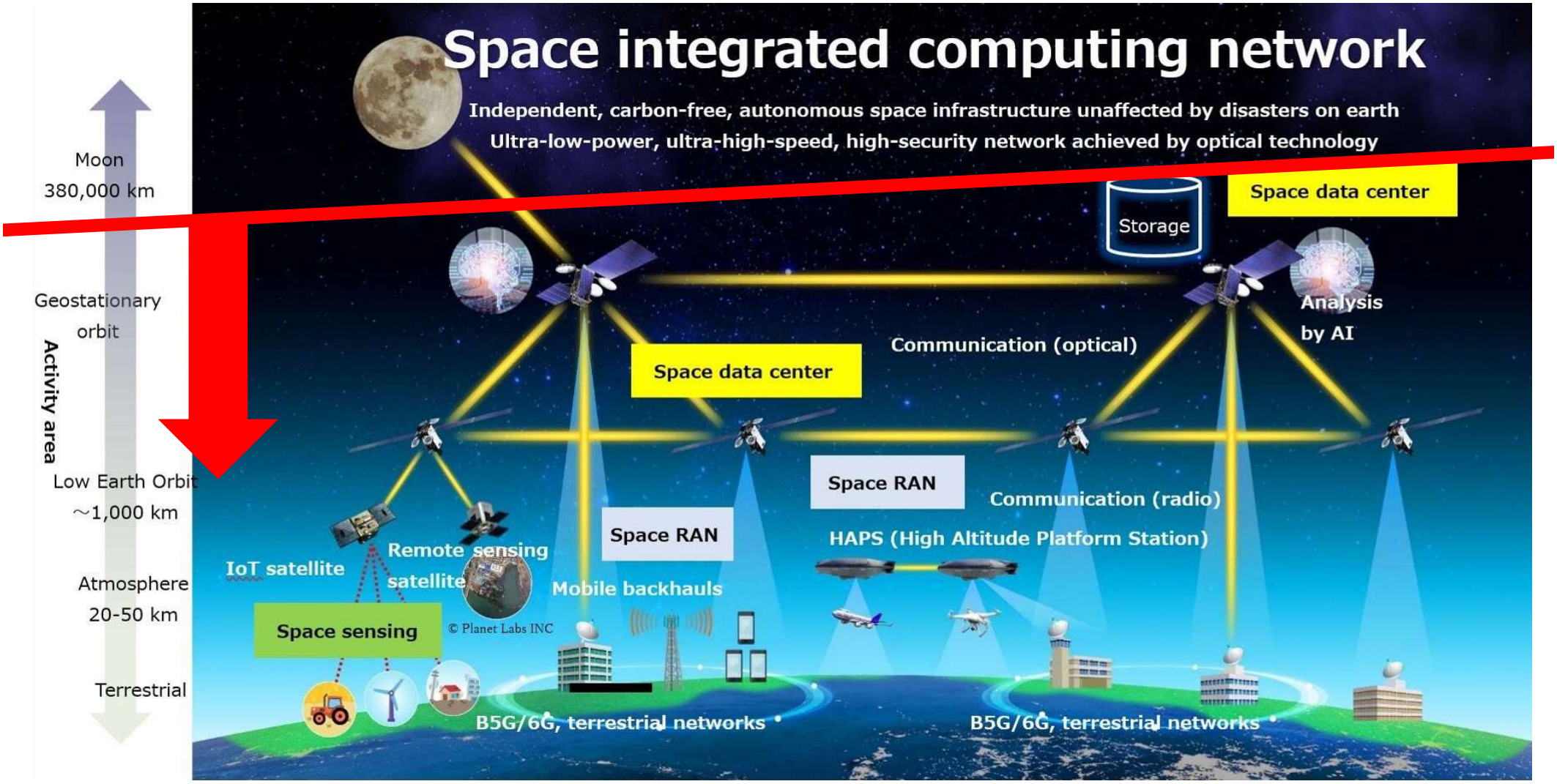
(Bild: NOIRLab/NSF/AURA/P. Marenfeld)

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

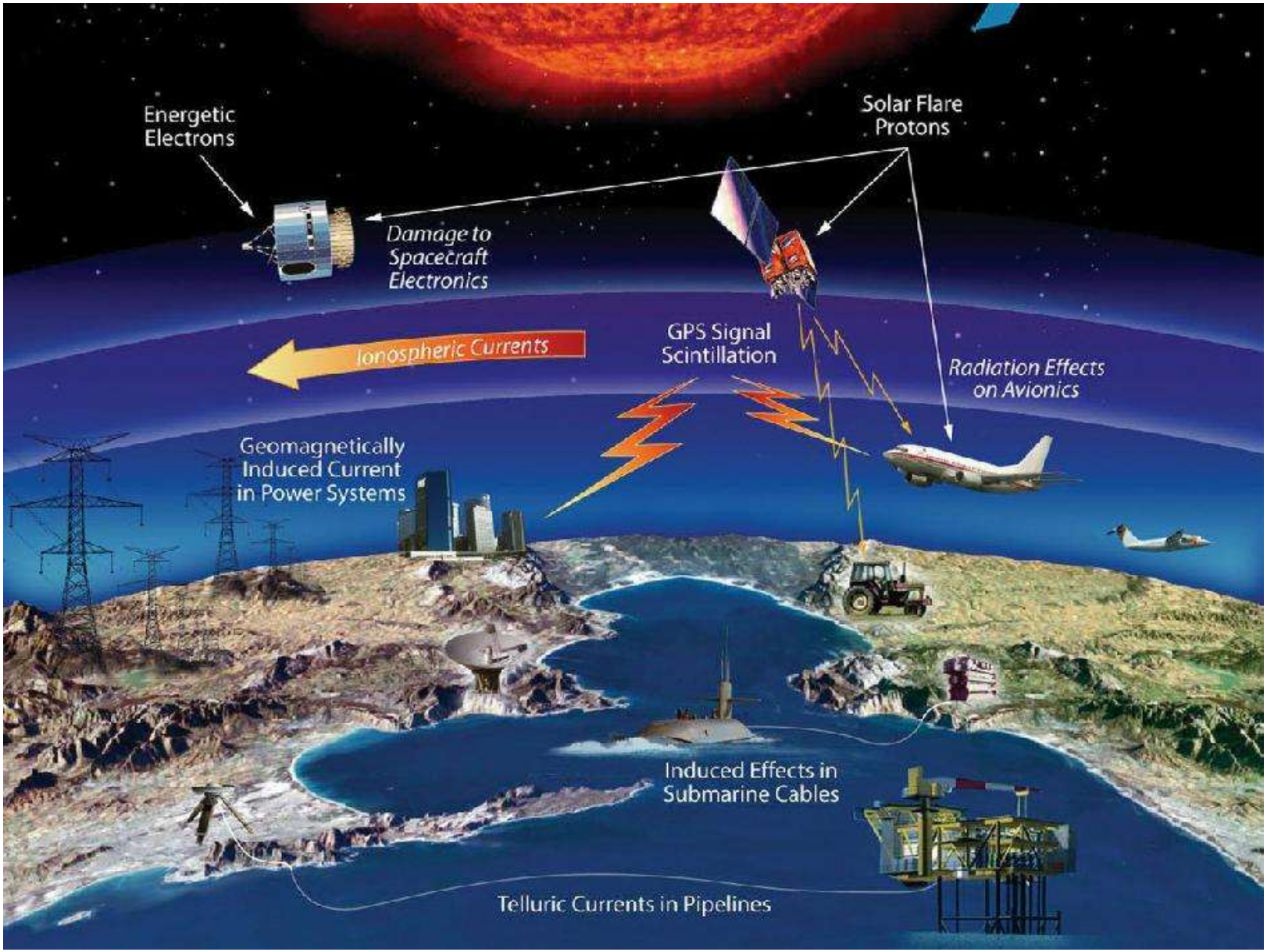
# Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



# Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



# Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



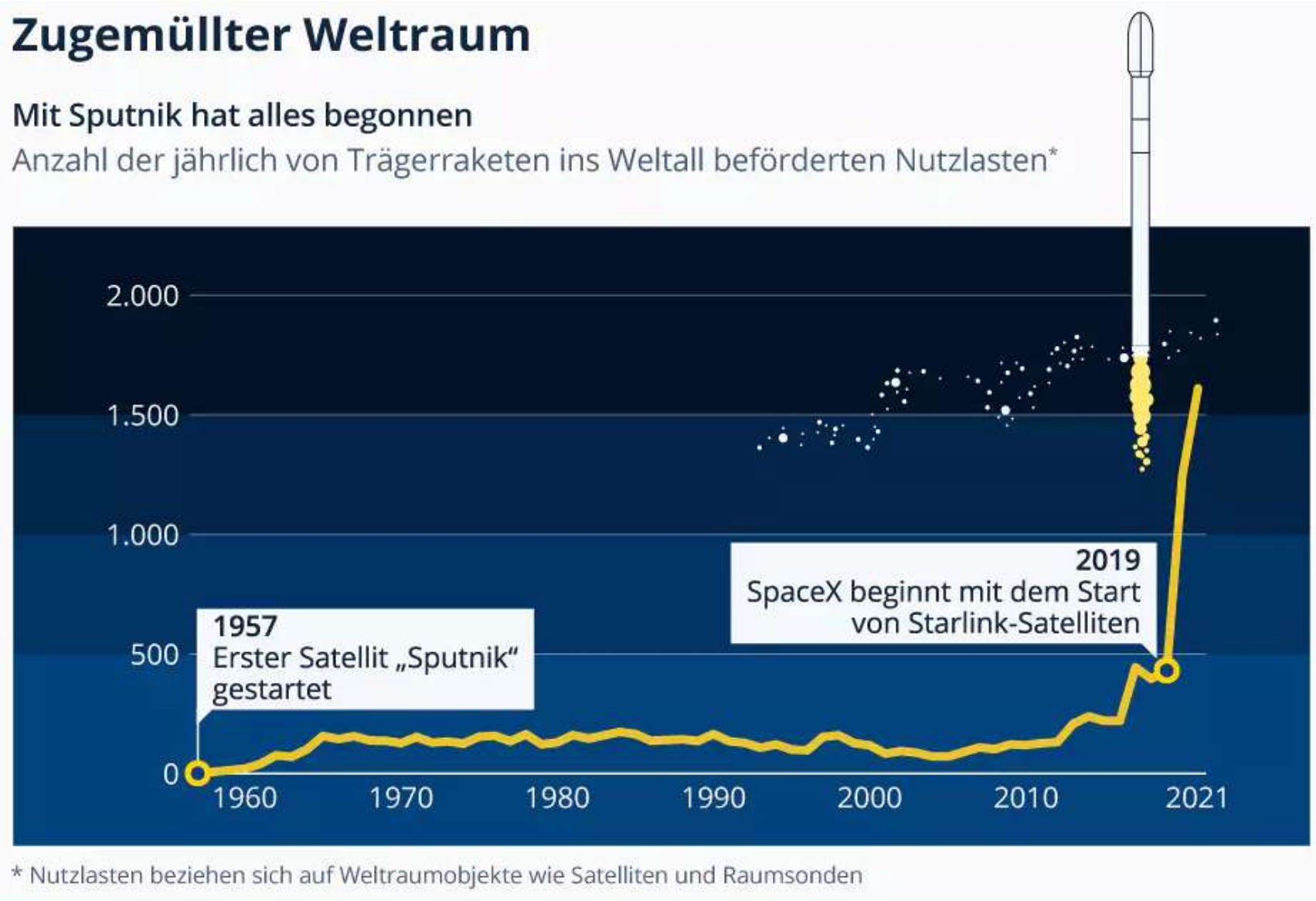
# Überblick 1: STATISTIKEN (2023)
## WELTRAUM-Objekte (gem. ESA)

## Space objects and debris by the numbers:

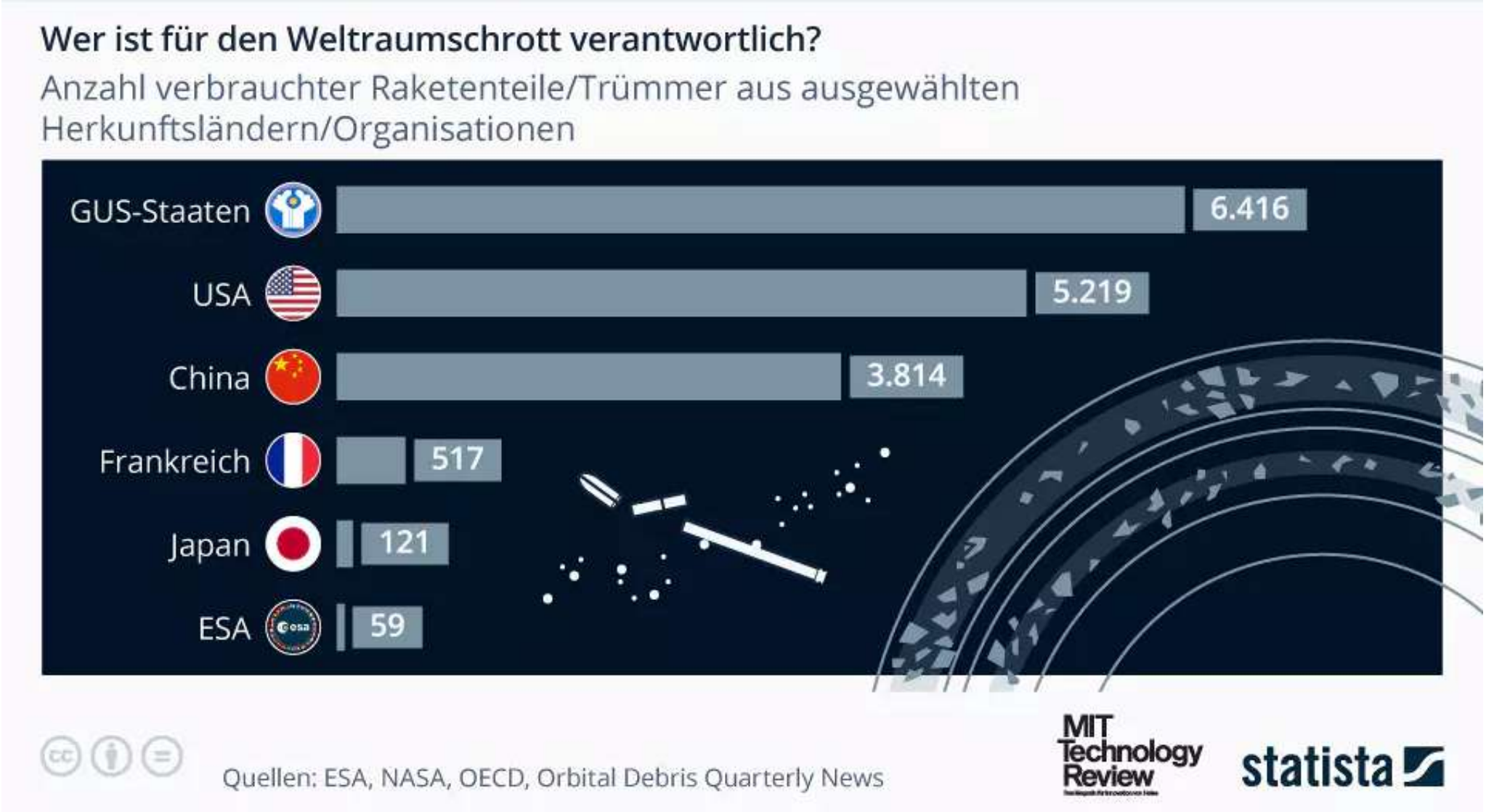
Number of **rocket launches** since the start of the space age in 1957:
**About 6500 (excluding failures)**
Number of **satellites these rocket launches** have placed into Earth orbit:
**About 16990**
Number of **satellites still in space:**
**About 11500**
Number of **satellites** still functioning:
**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**
**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**

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

# Überblick 2: STATISTIKEN (2023)
## WELTRAUM-Objekte (gem. statista)

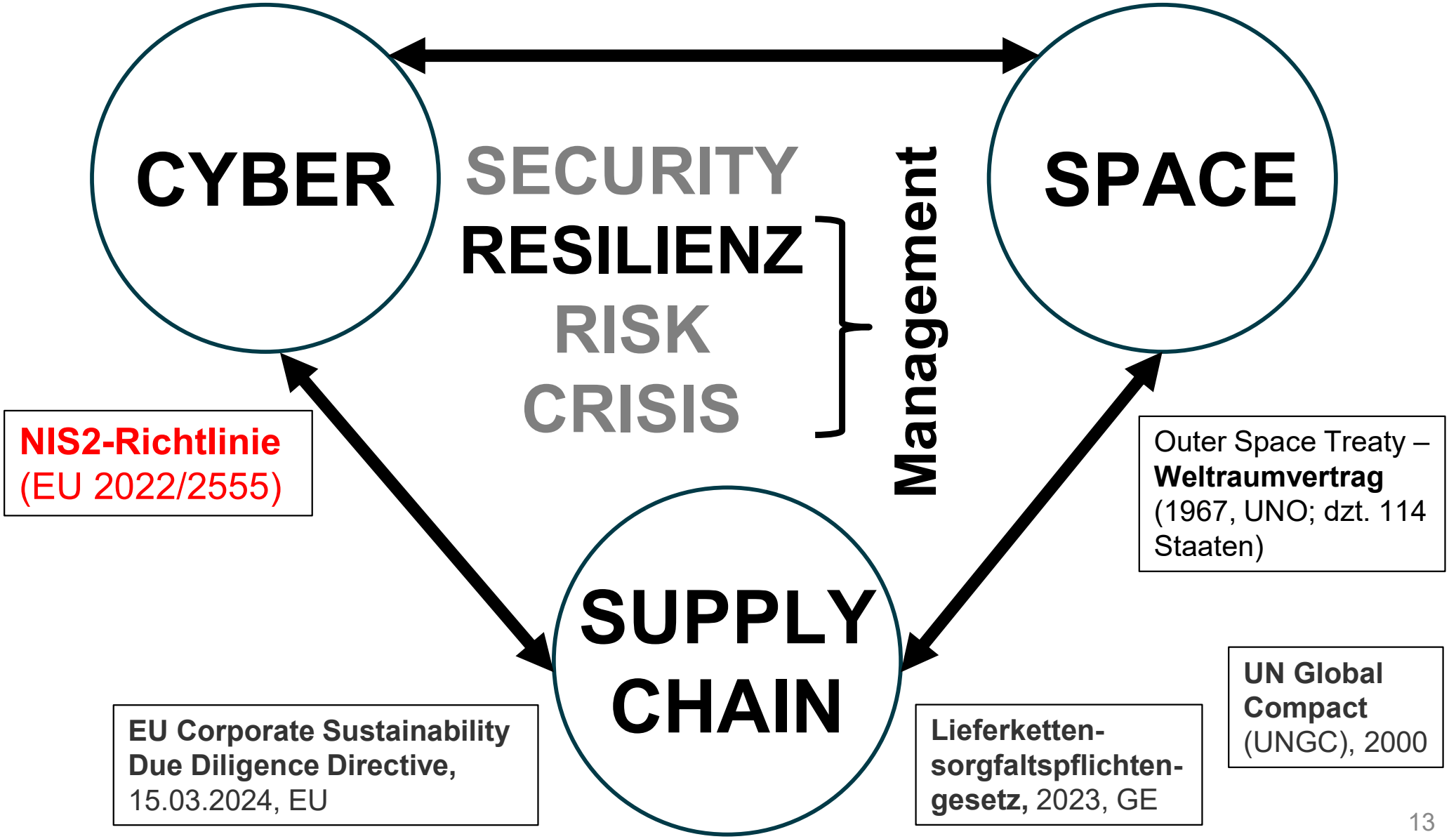


# Überblick 3: STATISTIKEN (2023)
## WELTRAUM-Objekte (gem. statista)



# 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

# Weltraum → Weltraumsysteme

**“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*

## Kommerzialisierung des Weltraums ("New Space")

- 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 Szenario-gestützter Cybersicherheit in das Management der bereits bestehenden hohen Operationsrisiken**

# Supply Chain Risks & Losses:

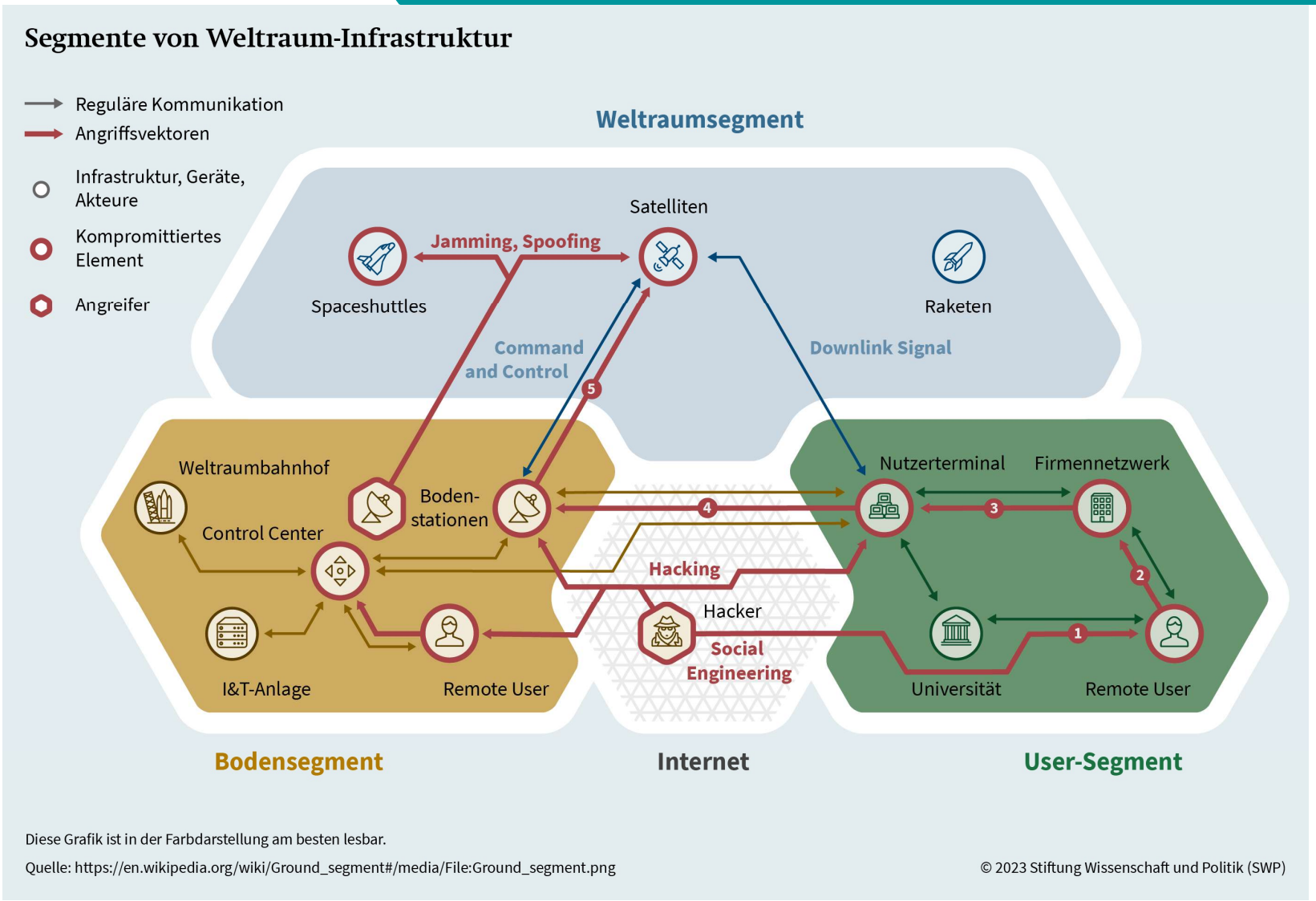
In framing financial discussions about losses due to supply chain risk, it is critical to analyze the operational impact of a disruption and the associated financial impact. Areas to look at include:

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*

# SUPPLY CHAIN RESILIENZ: Weltraum-Infrastruktur und Angriffsvektoren

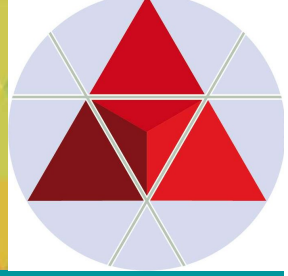



- ***Strukturmodell:*** Weltraumsystem als Ökosystem
- ***Schutzparadigma:*** Space-Air-Ground Integrated Network Security (SAGIN)



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

# 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**

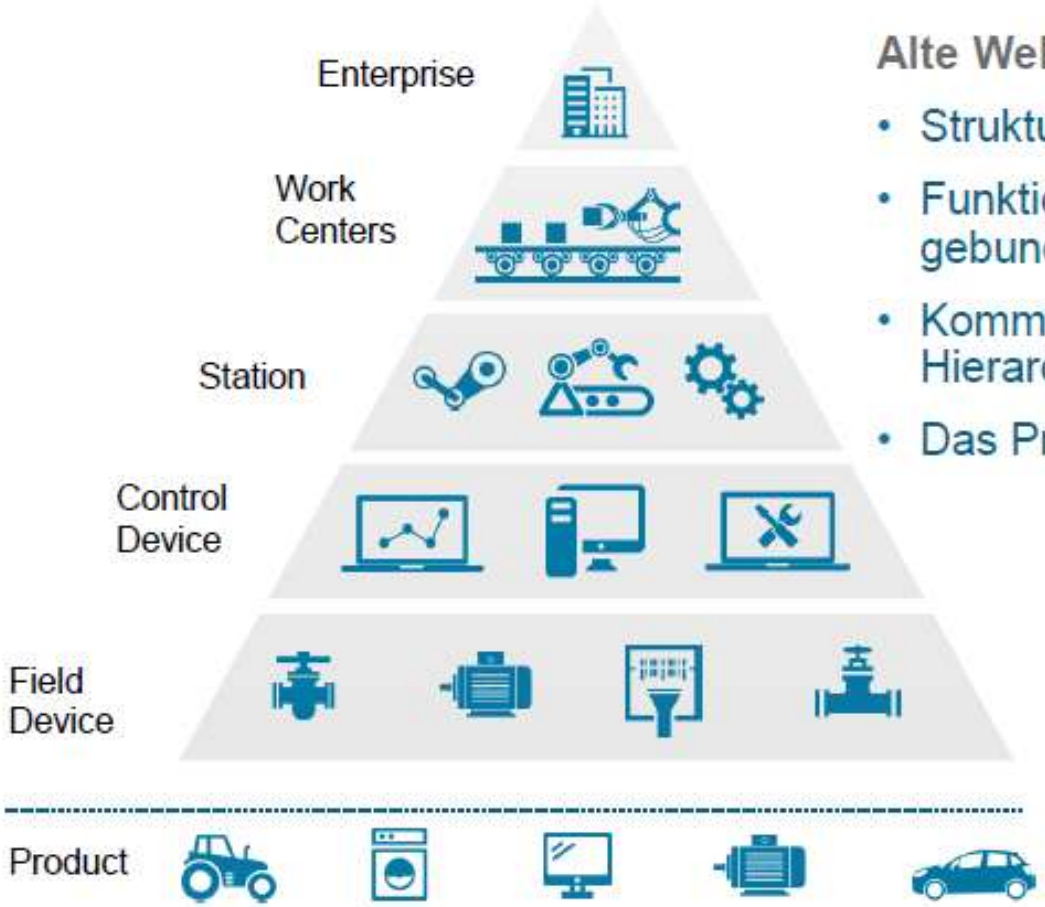
- Transport/Traffic-Networks
  - (Air, Road, Railway, Waterways)
- ICT-Networks (+/-: Smart Grids)
- Energy Networks (+/-: Smart Grids)

**III. Governmental & Public-/Administration Networks**

# KOMPEXITÄT für IKT in der Supply Chain

PLATTFORM INDUSTRIE 4.0

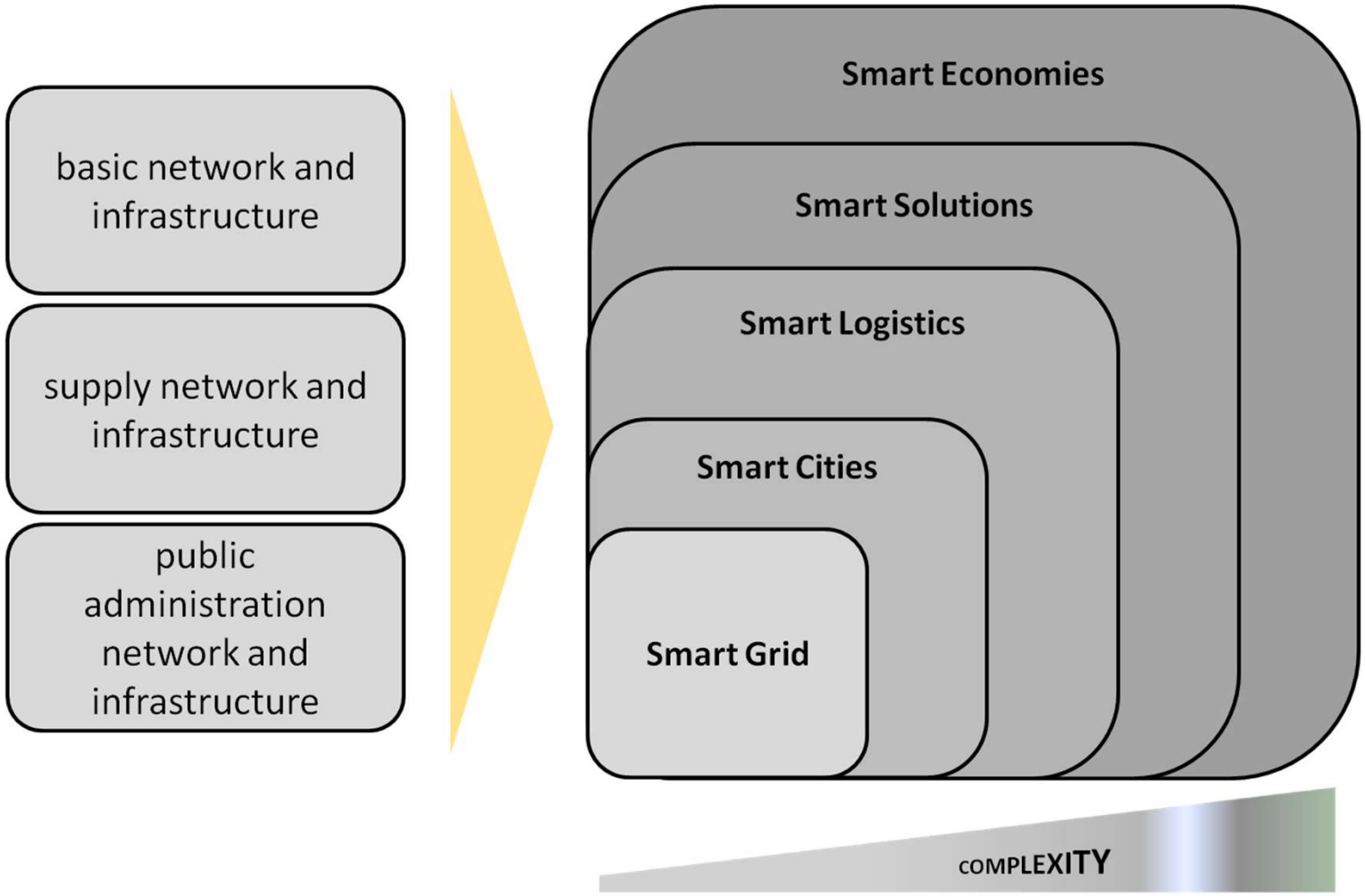
## Achse 1 – Hierarchie – Die Fabrik




**Alte Welt - Industrie 3.0**

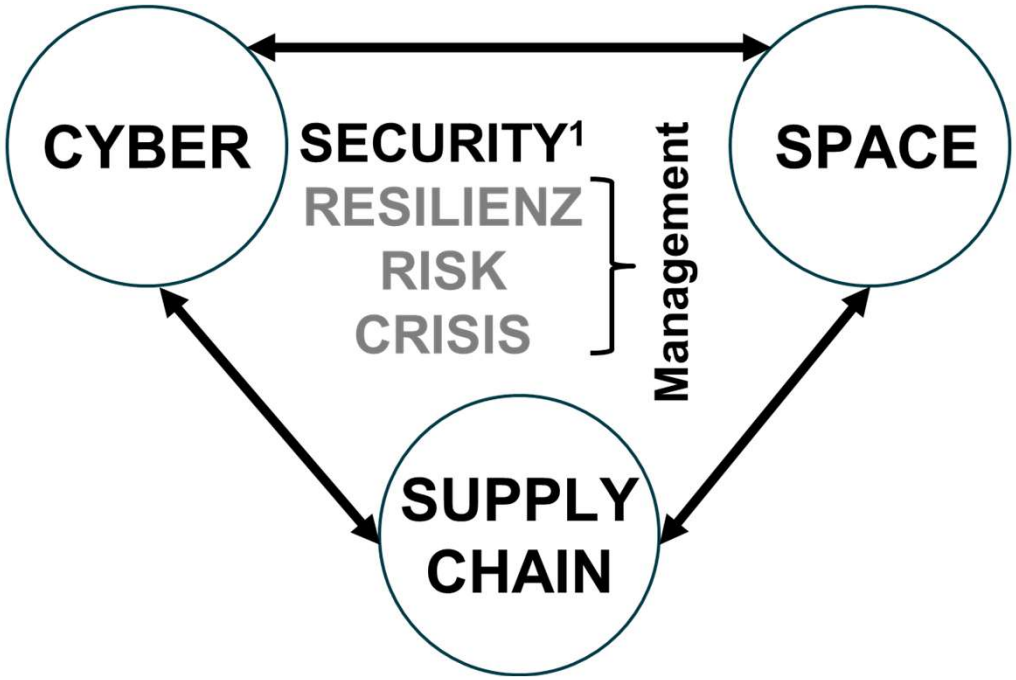
- Struktur durch Hardware
- Funktionen sind an Hardware gebunden
- Kommunikation zwischen Hierarchieebenen
- Das Produkt steht außerhalb

# 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)

# Outer Space Treaty – Weltraumvertrag

*(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**

# 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

# “All-hazards approach" : NIS 2 Directive

**Supply Chains ->** : Networks of Supply Chains

- *Erhöhte Komplexität*
- *Versteckte Single Points of Failure*
- *Steigenden Interdependenzen*

**Erhöhte Anhängigkeiten von Technologien**:

- Energie
- Kommunikation
- Finanzen
- Transport
- Information

Flooding of Rojana Industrial Park, Ayutthaya, Thailand, October 2011.jpg
http://en.wikipedia.org/wiki/File:Flooding_of_Rojana_Industrial_Park,_Ayutthaya,_Thailand,_October_2011.jpg



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

# Lieferkettensorgfaltspflichtengesetz

*(Deutschland, 1. Januar 2023 in Kraft getreten. Das Gesetz regelt die unternehmerische Verantwortung für die Einhaltung von Menschenrechten in den globalen Lieferketten.)*

**Das Gesetz stärkt in globalen Lieferketten Menschenrechte und den Umweltschutz**. Es verpflichtet Unternehmen in Deutschland zur Achtung von Menschenrechten durch die Umsetzung definierter Sorgfaltspflichten.

**Diese Pflichten gelten für den eigenen Geschäftsbereich, für das Handeln eines Vertragspartners und das Handeln weiterer (mittelbarer) Zulieferer. Damit endet die Verantwortung der Unternehmen nicht länger am eigenen Werkstor, sondern besteht entlang der gesamten Lieferkette.**

**Zunächst müssen Unternehmen die Risiken in ihren Lieferketten ermitteln, bewerten und priorisieren.** Aufbauend auf den Ergebnissen werden eine Grundsatzerklärung veröffentlicht und Maßnahmen ergriffen, um Verstöße gegen die Menschenrechte sowie Schädigungen der Umwelt zu vermeiden oder zu minimieren. Das Gesetz legt dar, welche Präventions- und Abhilfemaßnahmen notwendig sind. Zu den weiteren Pflichten gehören auch die Einrichtung von Beschwerdekanäle für die Menschen in den Lieferketten und die regelmäßige Berichterstattung über das Lieferkettenmanagement. Davon profitieren die Menschen in den Lieferketten, Unternehmen und auch die Konsumenten. Denn sie erhalten durch das Gesetz Rechtssicherheit und eine verlässliche Handlungsgrundlage für ein nachhaltiges Lieferkettenmanagement mit resilienten Beschaffungswegen. Den Verbraucher*innen bringt das Lieferkettengesetz die Sicherheit, dass insbesondere große Unternehmen in Deutschland nun einen noch stärkeren Fokus auf faire Herstellung legen müssen.



Source: Johannes GÖLLNER & Ralf HUBER, 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;*

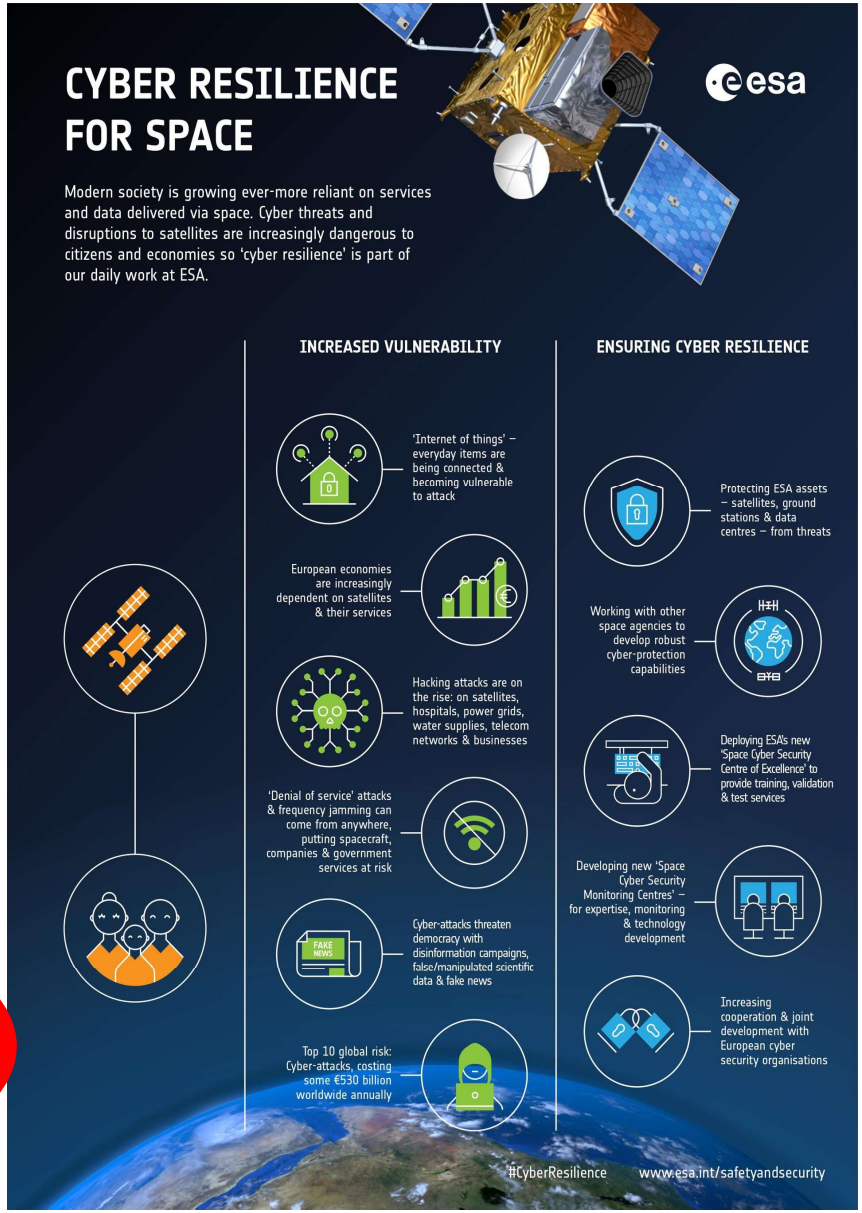
## Krisenmanagement: vs. BCM *(vgl. NIS 2)*

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

# 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




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

# 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

# Was soll NIS-2 gewährleisten?

1. **Stärkung der CYBER-Resilienz eines alle relevante Sektoren umfassendes Spektrum von Unternehmen,**

   - alle öffentlichen und privaten Einrichtungen im gesamten Binnenmarkt, die wichtige Funktionen für die Wirtschaft und die Gesellschaft als Ganzes erfüllen, sollen verpflichtet werden, angemessene Cybersicherheitsmaßnahmen zu ergreifen.

2. **Förderung einer gleich starken Resilienz bei den bereits unter die Richtlinie fallenden Sektoren im Binnenmarkt, durch weitere Angleichung**

   1. Des De facto Anwendungsbereiches,
   2. Der Sicherheitsanforderungen und Meldepflichten bei Sicherheitsvorfällen,
   3. Der Bestimmungen für die nationale Aufsicht und Durchsetzung sowie
   4. Der Kapazitäten der zuständigen Behörden in den Mitgliedstatten.

3. **Verbesserung der gemeinsamen Lageerfassung und der kollektiven Vorsorge und Reaktionsfähigkeit**

   1. Maßnahmen zur Stärkung des Vertrauens zwischen den zuständigen Behörden
   2. Verstärken des Informationsaustausches
   3. Festlegung von Regeln und Verfahren im Falle weitreichender Sicherheitsvorfälle oder Krisen.



Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

# NIS 2-Richtlinie (EU 2022/2555)

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

Gefährdungen  Bewältigungsmaßnahmen

"sichere Systemkonfiguration"
(system hardening)

- Vertraulichkeit – ("**C**onfidentiality")
- Integrität – ("**I**ntegrity")
- Verfügbarkeit – ("**A**vailability")

**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"

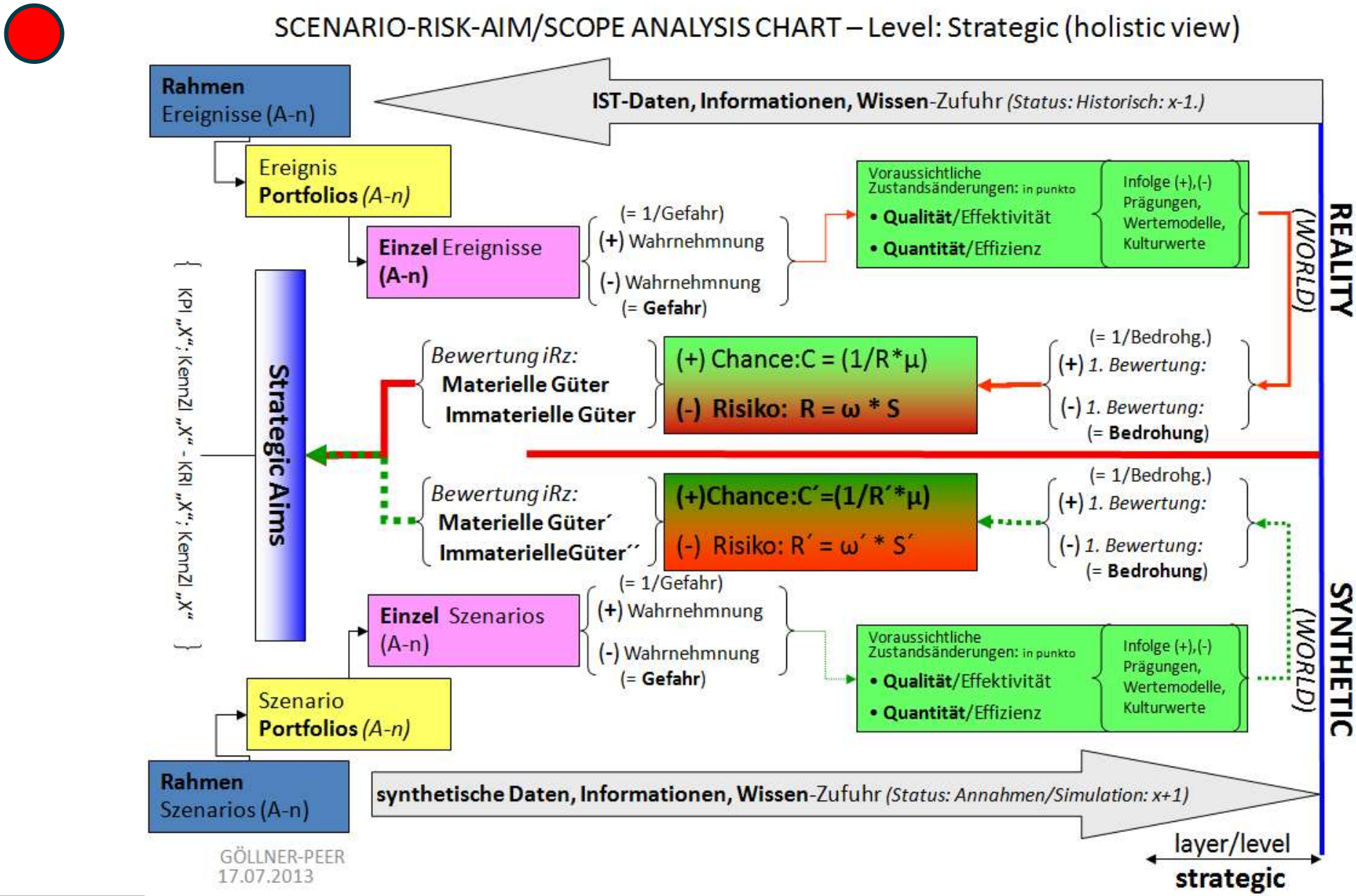
  - ***Öffentliche Verwaltung (neu)***
  - ***IKT-Dienste, einschließlich Cloud Computing Service (neu)***

- Kriterium: Gefahr von Kaskadeneffekten

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

# RISK MODELING
# &
# PERFORMANCE
# MONITORING SYSTEM

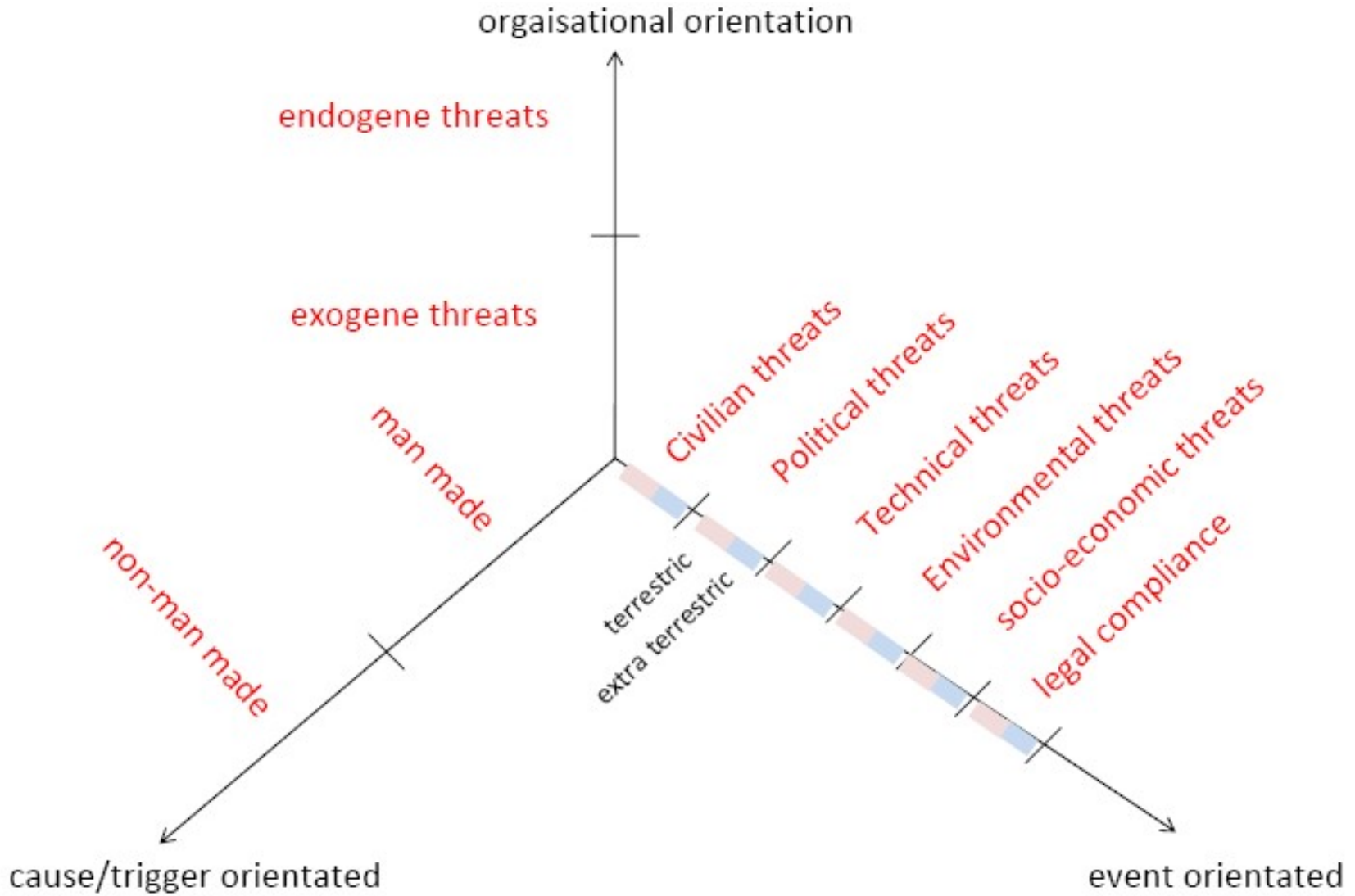
# Towards an integrated model: „RMPMS: Supply Chain-CYBER/ICT-SPACE “






Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

# Meta Model of an Organisation



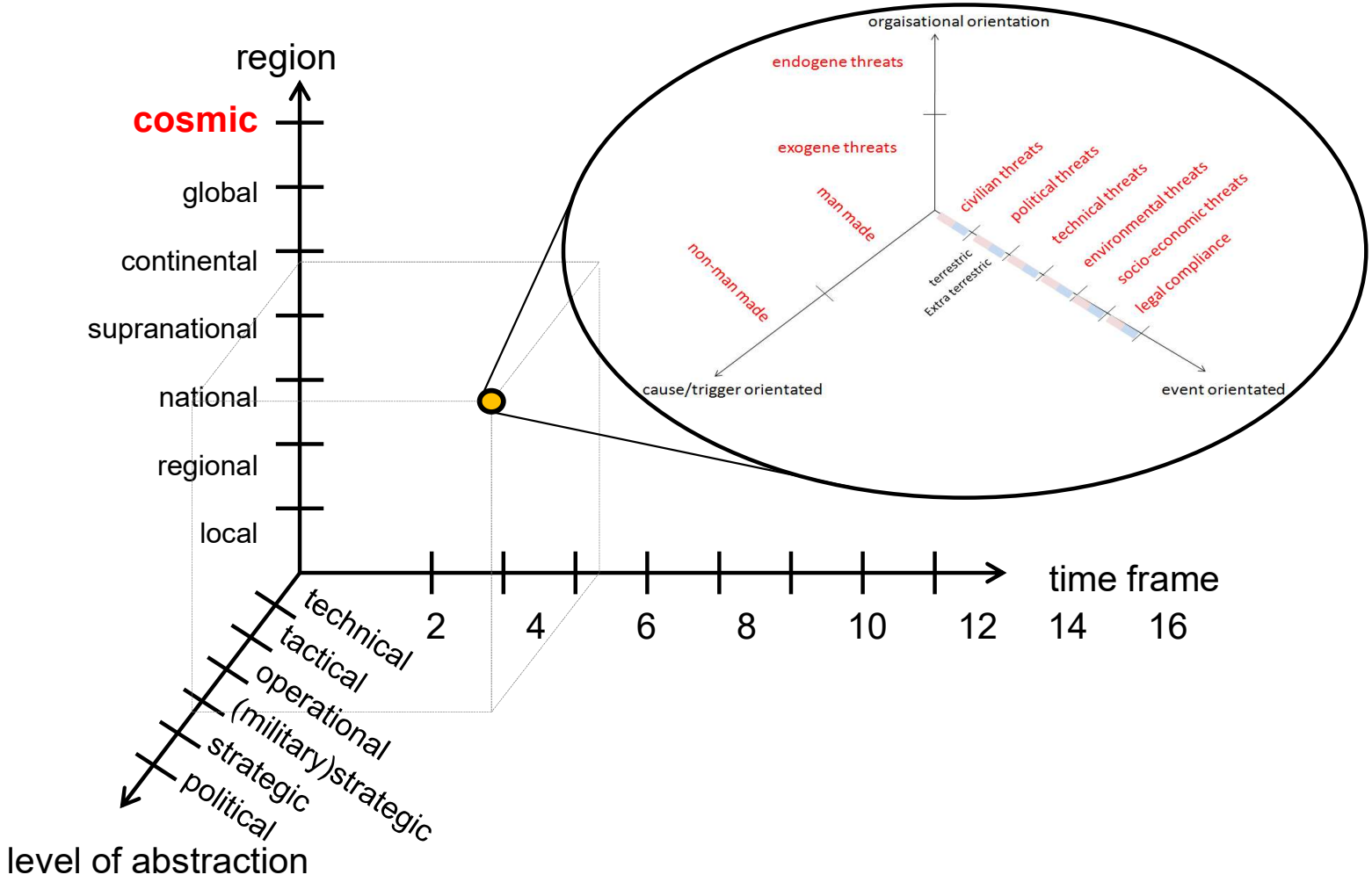







Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

# Multilayer Vector Model - Basis for Decision Making




Quelle: Copyright by Zentraldokumentation/ Landesverteidigungsakademie, Wien, 12/2010 und 10/2011 (GÖLLNER, MAK, PEER, POVODEN)



Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

# RMA-LEITFADEN:

## „Supply Chain Resilience Management“

# Lösungsansätze: Beitrag RMA e.V., AK SCRM

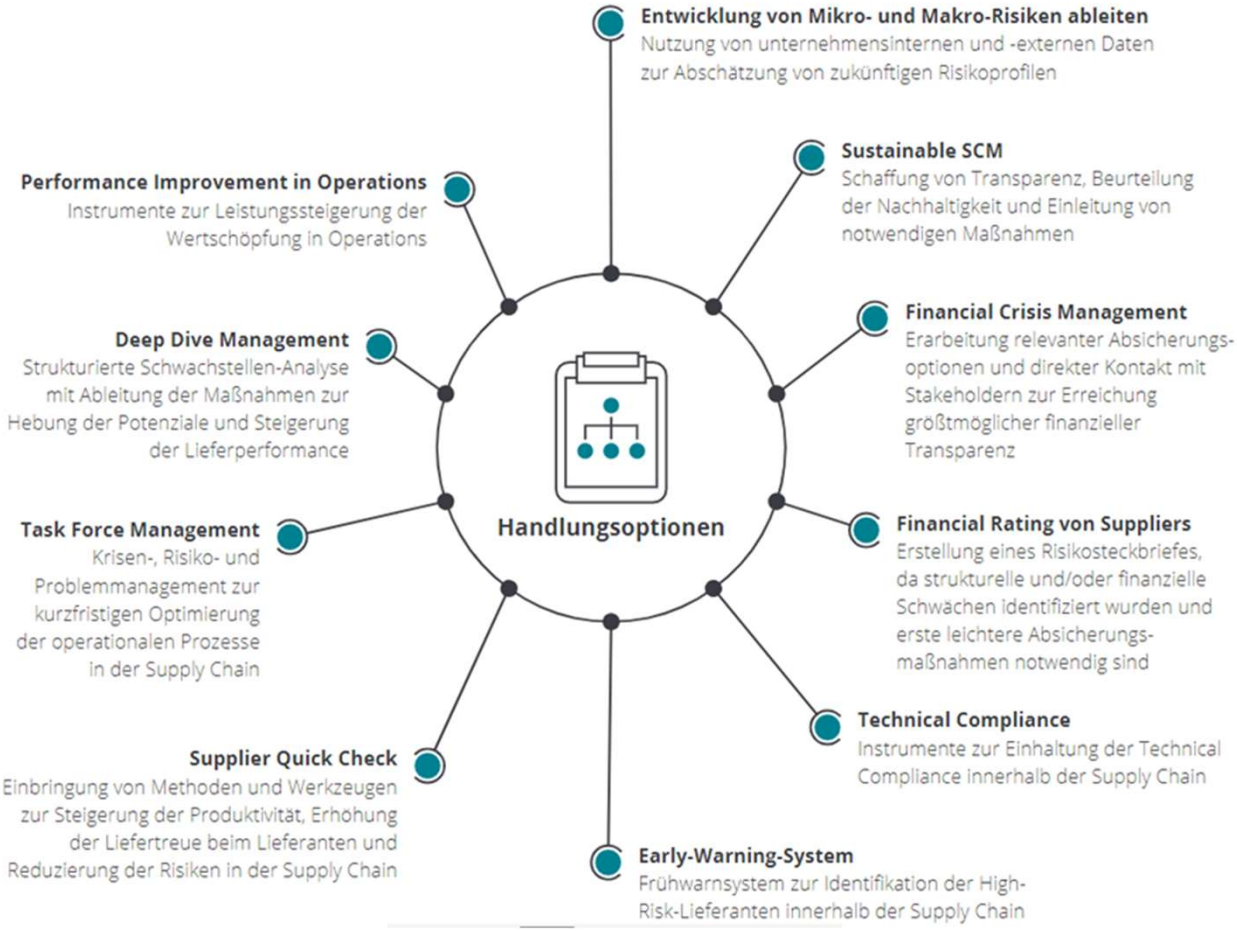
## RMA-Leitfaden: SUPPLY CHAIN RESILIENZ MANAGEMENT




Source: Johannes GÖLLNER, Ralf A. HUBER, Prof. Ulrike LECHNER, Sonja REMSCHEL, Alle: RMA AK SCRM-Kernteam, 2023

# Lösungsansätze: Beitrag RMA e.V., AK SCRM

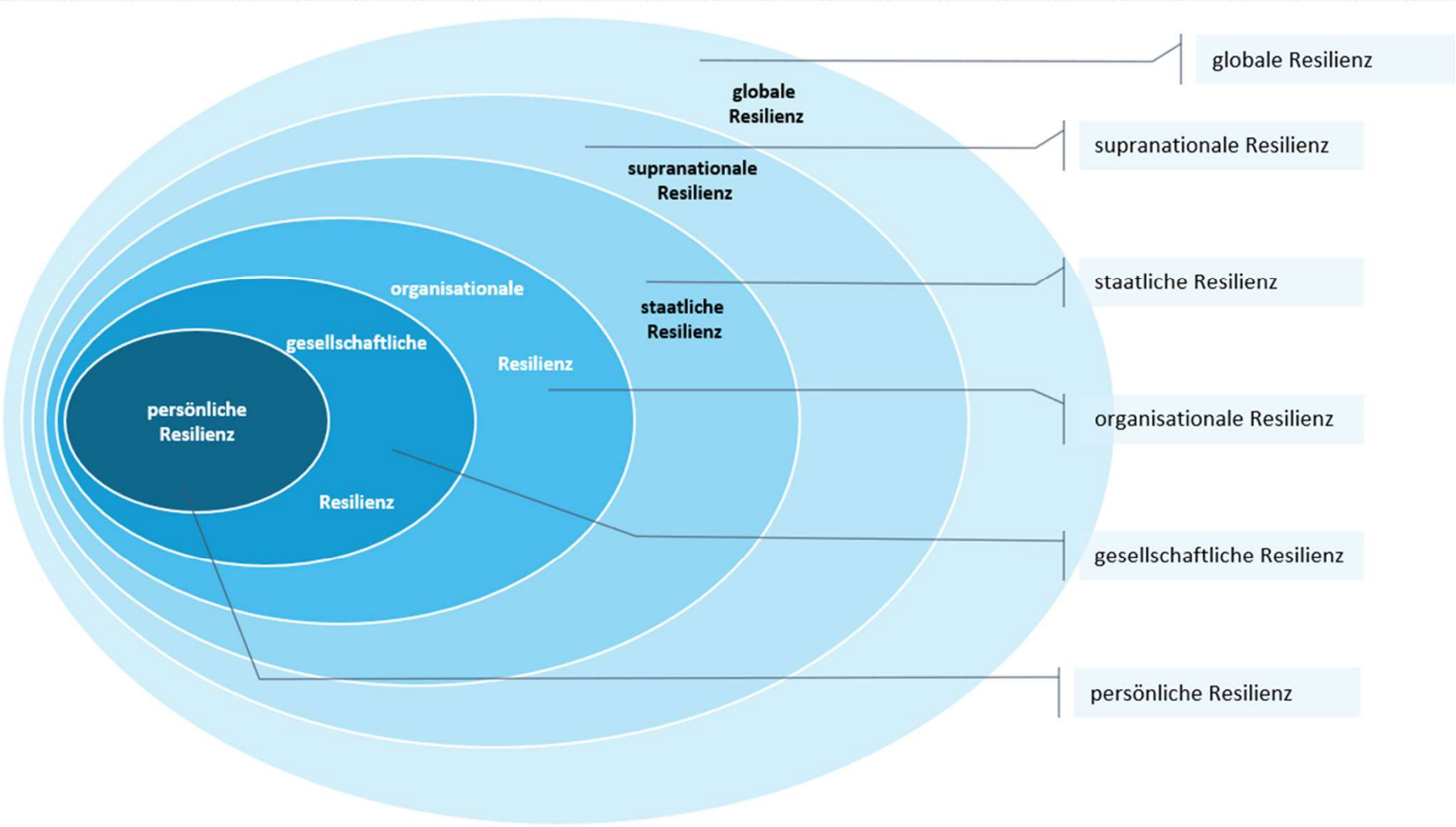
## RMA-Leitfaden: Veröffentlichung: 10/2025 (expected)
## SUPPLY CHAIN RESILIENZ MANAGEMENT




Source: Deloitte, 2023

# FAZIT & AUSBLICK:

## Strategische Resilienz:

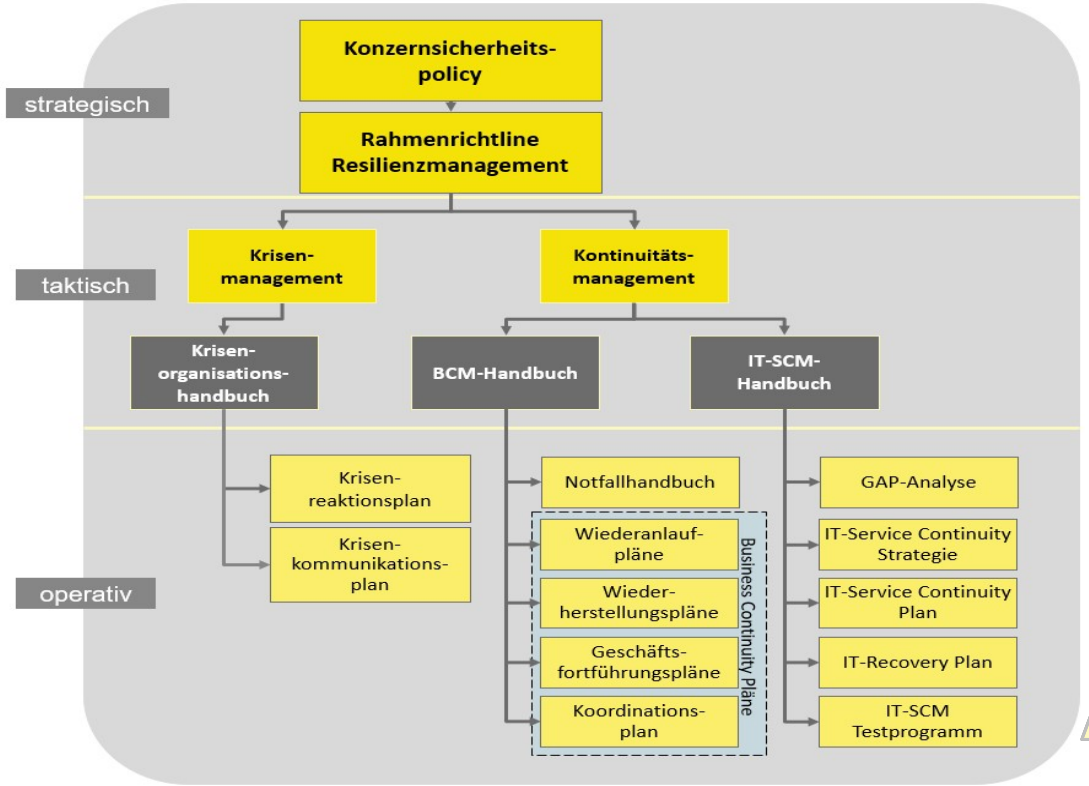


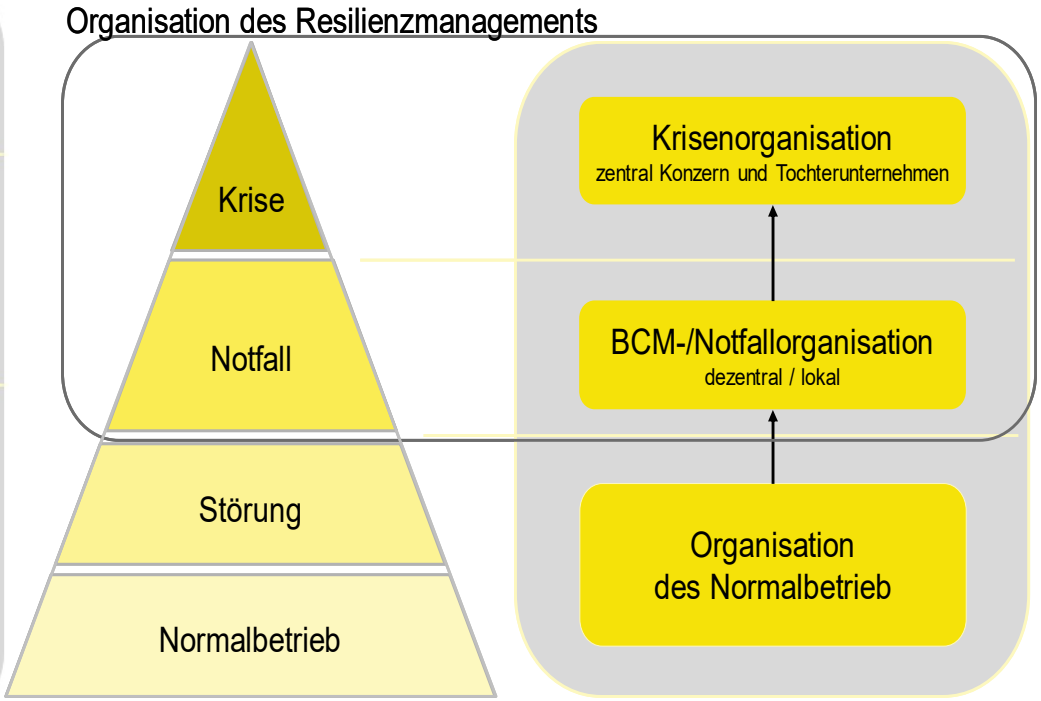

Zentrum für Risiko- & Krisenma

Quelle: Christian Paul, Johannes Göllner, et al – ZRK-Positionspapier: Strategische Resilienz

# FAZIT & AUSBLICK:

## Implementierung **Resilienzmanagement**:




*Quelle:* Christian Paul, BSc MA, Post AG / IKT Sicherheitskonferenz 2023, 03.10.2023, 17:20, Linz, Österreich, link: ProgKonferenz.pdf (bundesheer.at)

# FAZIT & AUSBLICK:

1. **Grünbuch: „STRATEGISCHE RESILIENZ“** (D-A-CH)

2. ***VSSC 2025-STRATEGIC RESILIENCE-ENQUETE am 10.11.2025, Wien***

3. ***VSSC 2026 am 07.05.-08.11.2025, Wien***



Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

# Kontakte


## Johannes L. GOELLNER

**Vorstandsvorsitzender**
**Zentrum für Risiko- und Krisenmanagement,** Wien
*email:* johannes.goellner@zfrk.org
*mobil:* +[43]-650-2252991

**Vorstandsmitglied RMA e.V. &**
**Leiter RMA-AK-SCRM**
www.rma-ev.org, *München*

## Ralf A. HUBER

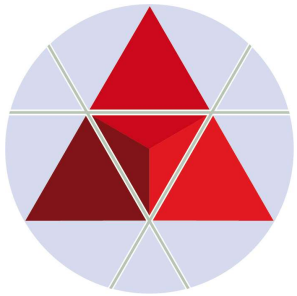
**Compliance & Risk Management**
**STAEDTLER SE**

www.staedler.com , *Nürrnberg*
*email:* ralf.huber@staedtler.com
*mobil:* +[49]-163-9809054

**Vorstandsmitglied RMA e.V. &**
**Mitglied des RMA-AK-SCRM**
www.rma-ev.org, *München*

**Stiftungsratsmitglied**
**Funk Stiftung**

www.funk-stiftung.org , *Hamburg*



Zentrum für
Risiko- & Krisenmanagement

# Thank you for your attention.

excellent.
connected.
individual.