RMA
Risk Management & Rating Association e.V.

Zentrum für
Risiko- & Krisenmanagement

RMC 2024
Hamburg, 13.05.2024, 14:30-15:15 Uhr

Kritische SPACE und CYBER Infrastruktur Risiken für die Supply und Value Chain

- **Dipl.-Ing. Johannes GÖLLNER, MSc**
  (RMA e.V., München & ZRK, Wien)
- **Ralf A. HUBER**
  (RMA e.V., München)

excellent.
connected.
individual.

AGENDA:

1. PRESSEMELDUNGEN
2. SUPPLY CHAIN RESILIENCE
3. REGULATORIK
4. RISK MODELING & PERFORMANCE MONITORING SYSTEM
5. BILDUNG
6. RMA-LEITFADEN: „SUPPLY CHAIN RESILIENCE MANAGEMENT
7. FAZIT & AUSBLICK

PRESSE-MELDUNGEN

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

WELTRAUMSCHROTT

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.

PRESSEMELDUNGEN: SUPPLY CHAIN & CYBER

Zurück

Dienstag, 09.04.2024

Seite 2 von 28

2 RESILIENZ contentway

RESILIENZ

contentway

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.

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

Resilienz ist mehr als Krisenmanagement

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

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

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-

ırück

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

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: Kompetenzen

IT-Fachkräftemangel: Herausforderungen und Lösungsansätze für Unternehmen

Viele Unternehmen, Organisationen und Behörden stehen vor der Herausforderung, offene Stellen im IT-Bereich zeitnah zu besetzen. Laut Bitkom blieben im Jahr 2023 149.000 Positionen in der IT-Branche unbesetzt. In Anbetracht dessen müssen Unternehmen kreative Lösungen entwickeln, um Fachkräfte anzuziehen.

Denn eine gut funktionierende und sichere IT-Infrastruktur ist entscheidend für die zukünftige Wettbewerbsfähigkeit. Spezialisierte Personalagenturen, die sich ausschließlich auf den IT-Bereich fokussieren, können hier eine äußerst wertvolle Option darstellen. Gudrun Müller, CEO

Gudrun Müller,

Fachkräften bei der Umsetzung ihrer IT-Projekte unterstützen. Hierzu bedi nen wir uns unseres eigenen Netzwerk aber auch der internationalen Datenbank unserer irischen Muttergesellschaft Cpl.

Prüfen Sie jeden Experten persönlich, bevor sie diese ihren Kunden vorstelle

Ja. Die Mehrheit unserer Kunden benötigt möglichst schnell nach der Anfrage einen oder mehrere passende IT-Experten. Mit passend meinen wir nicht nur, dass die gefor

Unternehmen brauchen Krisenmanag

SUPPLY CHAIN

Huthi-Rebellen bedrohen gerade Transportschiffe von Ländern, die Sympathien für Israel bekunden. Doch Lieferketten, Waren und Menschen sind auf noch weiteren Ebenen gefährdet.

Text: Katja Deutsch
Foto: Andreas Dittberner/unsplash, Presse

Ein Großteil der Unternehmen in Deutschland hat seine Produktionsstandorte im (meist weit entfernten) Ausland und damit in den letzten Jahrzehnten entsprechend

den Welthandel – was insbesondere deutsche Unternehmen zu spüren bekommen. Auf dem Seeweg von Asien nach Europa meiden deshalb viele Containerschiffe inzwischen den kur-

> *Unternehmen sollten ein professionelles Krisenmanagement betreiben und auf Flexibilität in der Lieferkette achten – nicht nur bei den Transportwegen, sondern auch bei den Lieferanten selbst.*

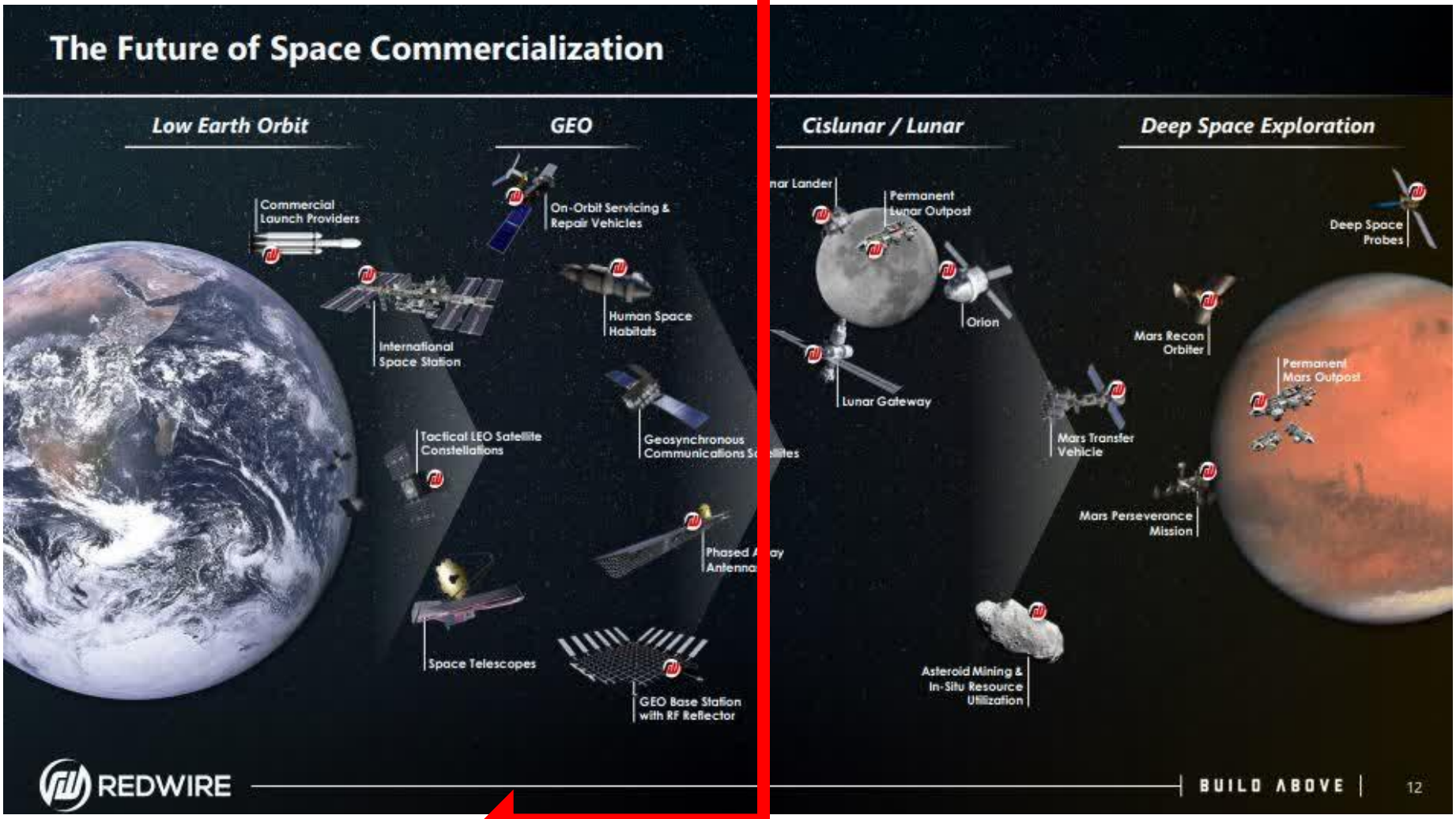
> *Um die Warenverfügbarkeit sicherzustellen, ist es ratsam, mögliche plötzliche Veränderungen entlang der Lieferketten Punkt für Punkt zu visualisieren und zu verändern.*

Ausnahmezustand an der Falkenstrasse: Ein Ransomware-Angriff erschüttert die NZZ-Gruppe in ihren Grundfesten.

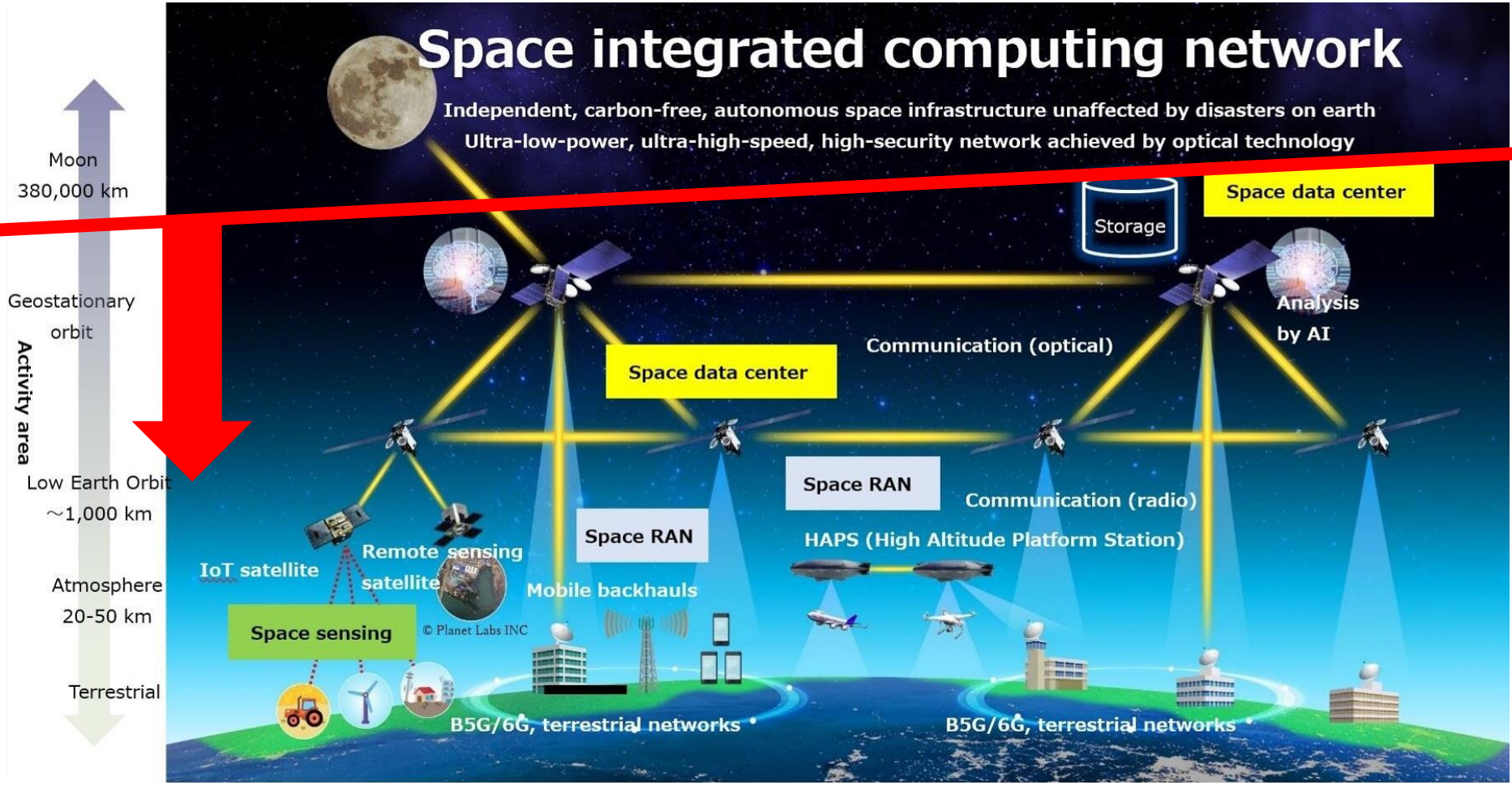
Und plötzlich bricht die IT der Zeitung zusammen

Im März vor einem Jahr wird die NZZ von kriminellen Hackern angegriffen und erpresst. Die Folgen beschäftigen das Medienhaus über Wochen und Monate. Dabei hat der Verlag noch Glück. VON LUKAS MÄDER

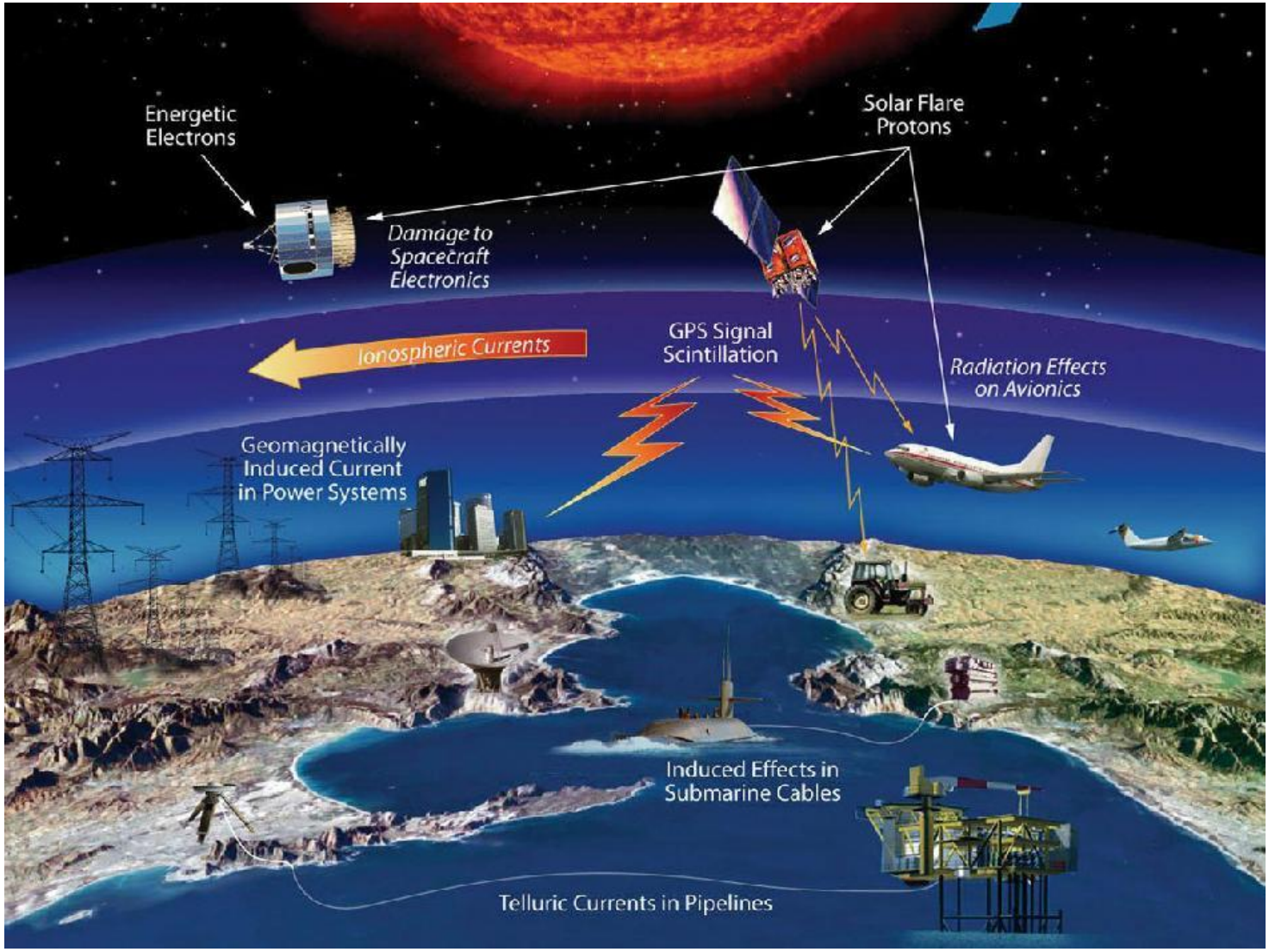
Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



Terestric & Space Infrastructure (SUPPLY CHAIN NETWORK)



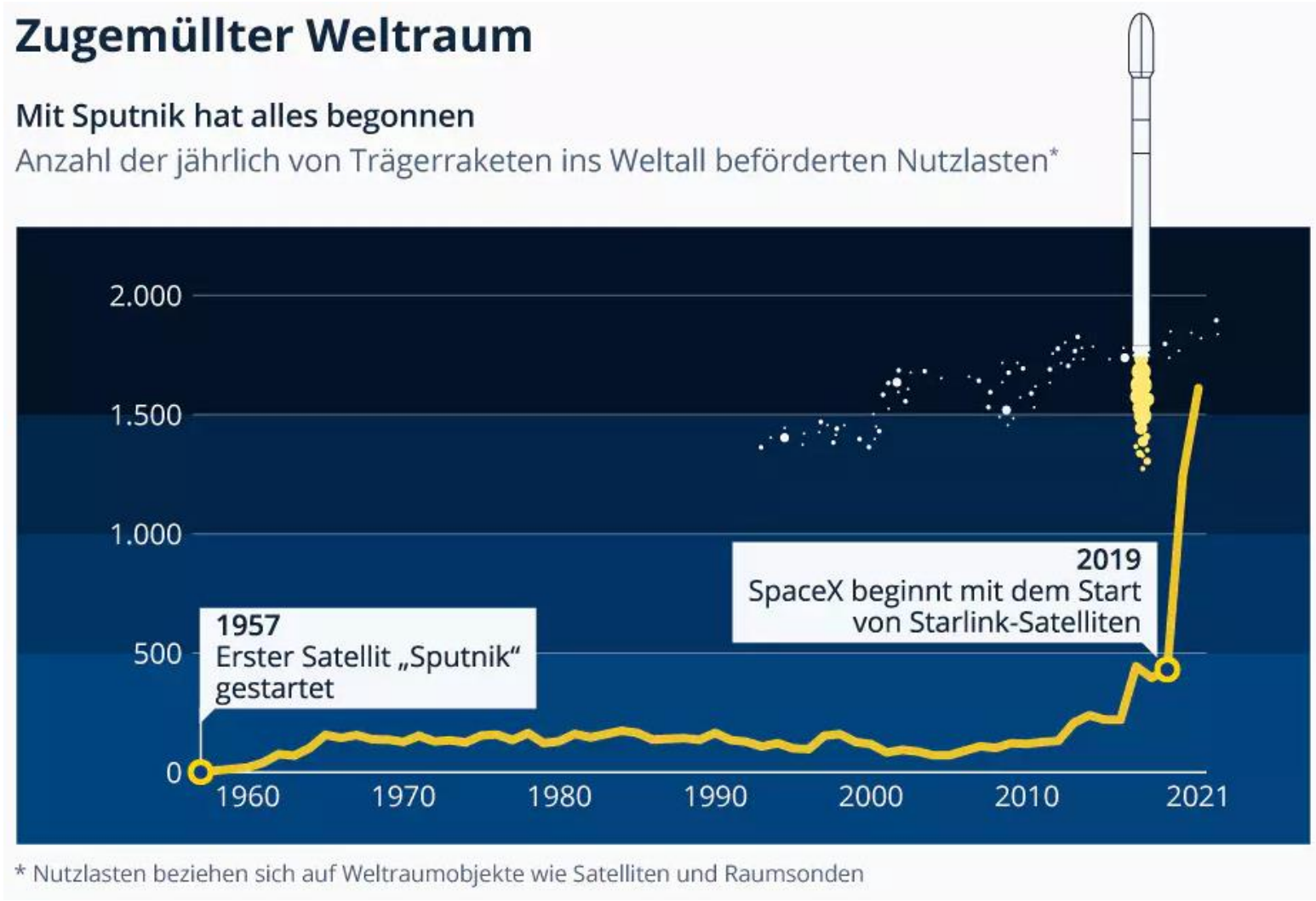
Überblick 1: STATISTIKEN (2023)
WELTRAUM-Objekte (gem. ESA)

Space objects and debris by the numbers:

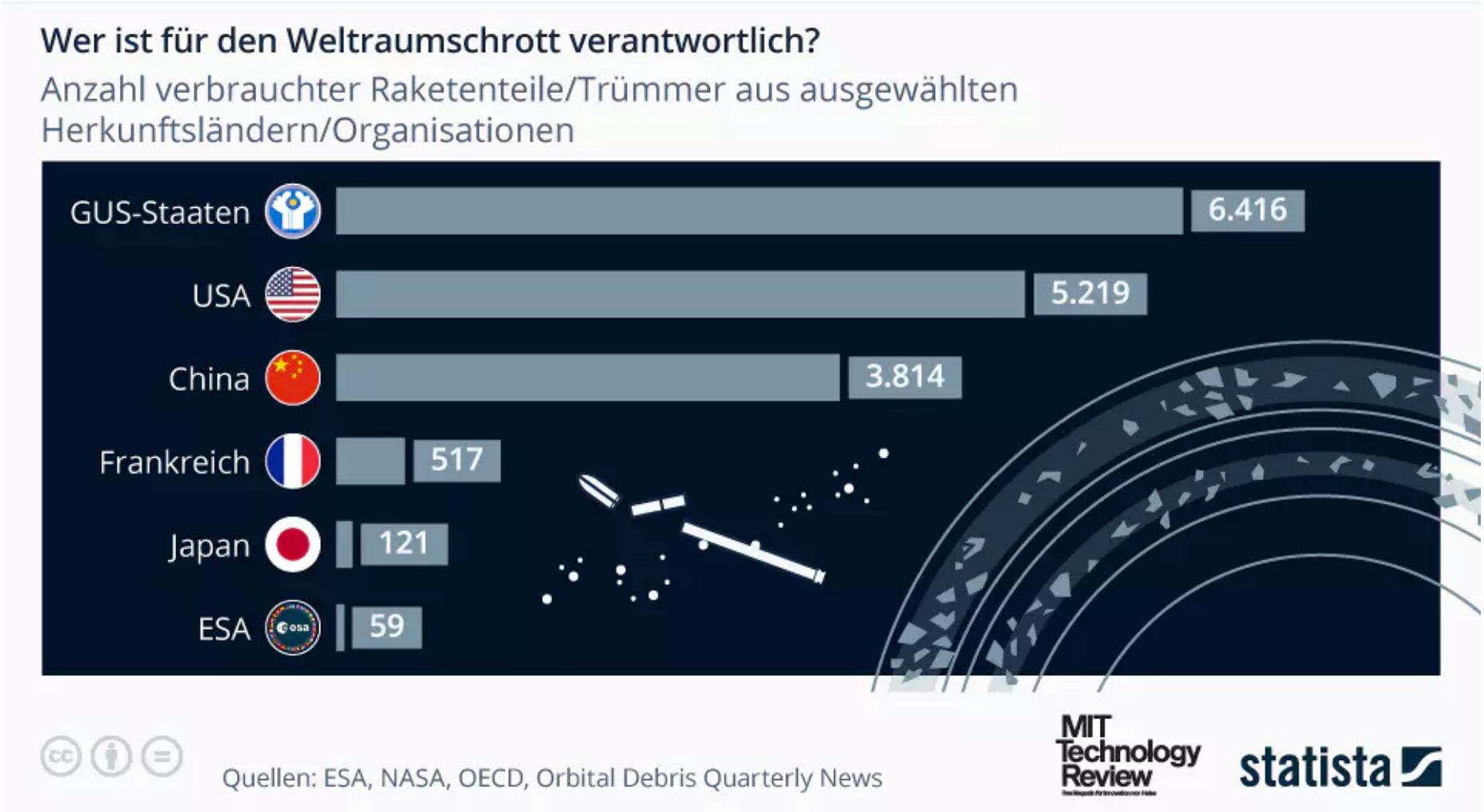
Number of **rocket launches** since the start of the space age in 1957:
About 6500 (excluding failures)
Number of **satellites these rocket launches** have placed into Earth orbit:
About 16990
Number of **satellites still in space:**
About 11500
Number of **satellites** still functioning:
About 9000
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)

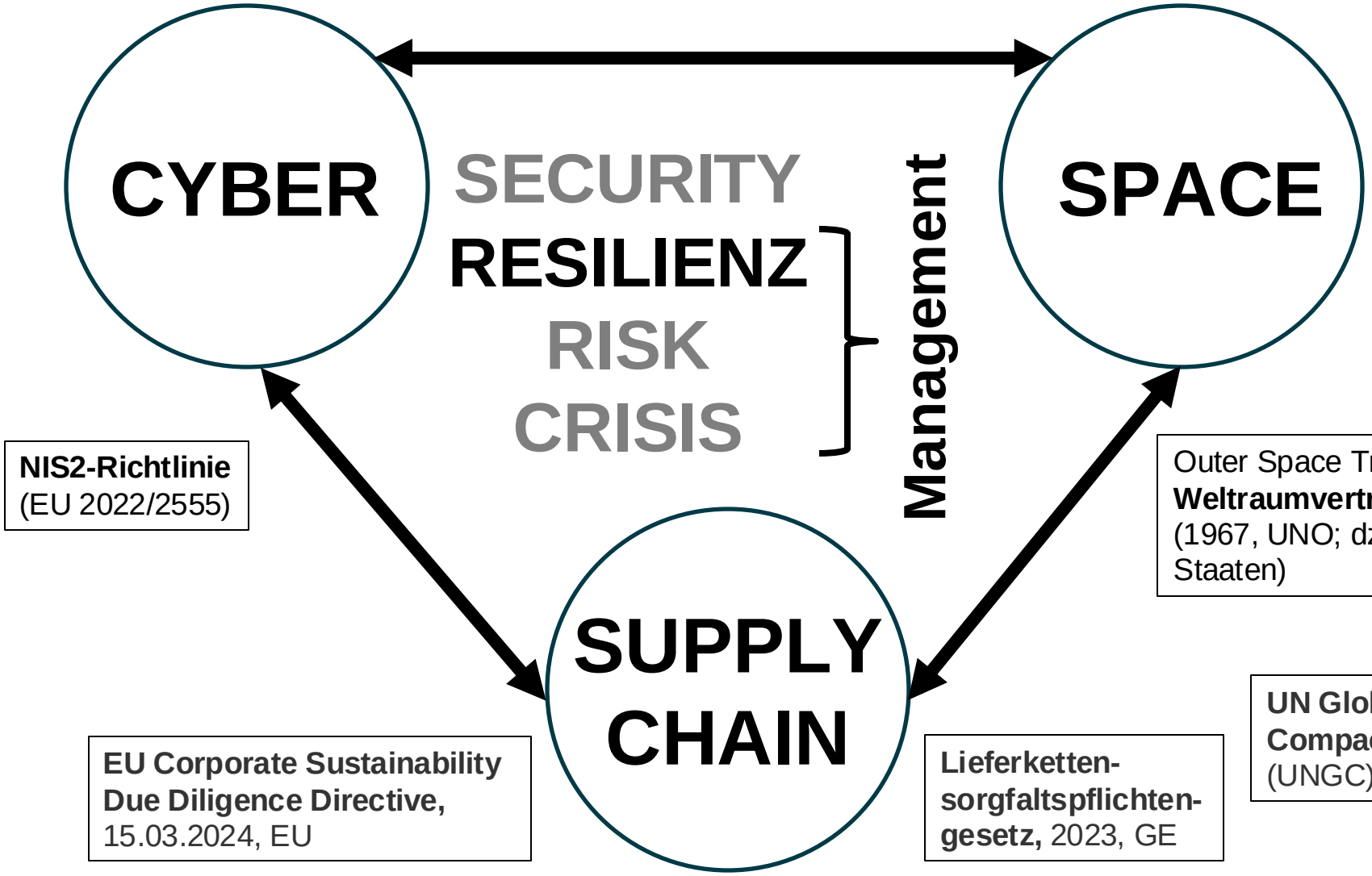


Überblick 3: STATISTIKEN (2023)
WELTRAUM-Objekte (gem. statista)



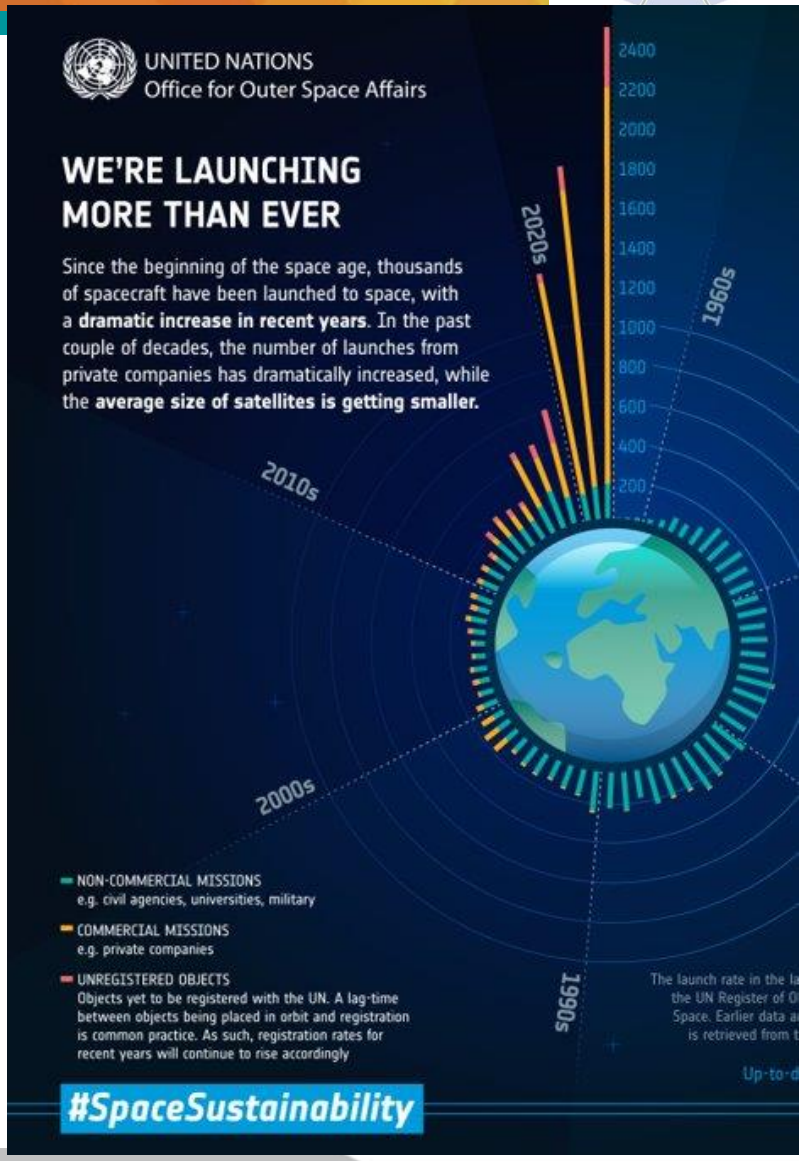
SUPPLY CHAIN RESILIENCE

SUPPLY CHAIN RESILIENZ



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: 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**%))

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:

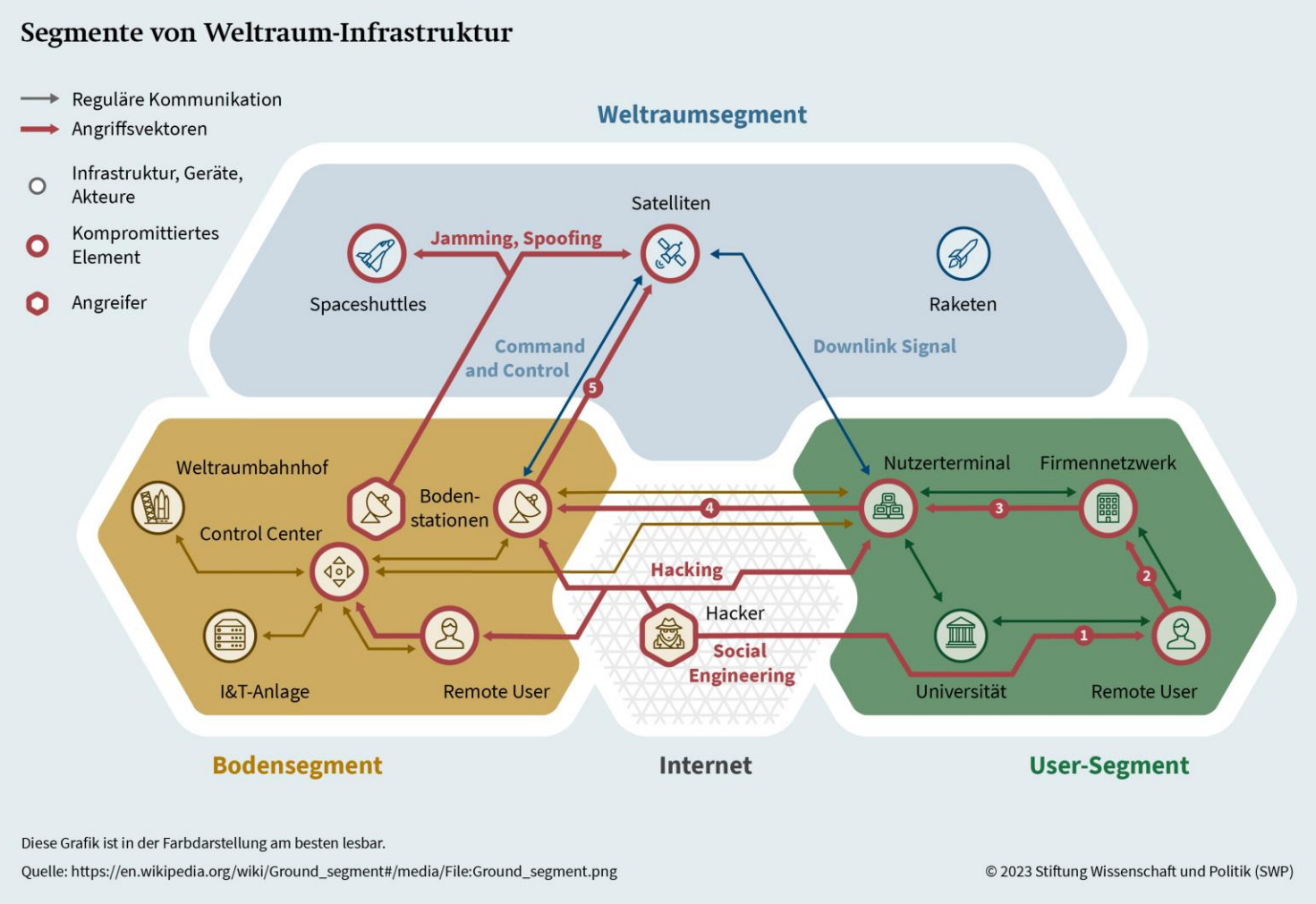
In framing financial discussions about losses due to supply chain risk, it is critical to analyze the operational impact of a disruption and the associated financial impact. Areas to look at include:

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)

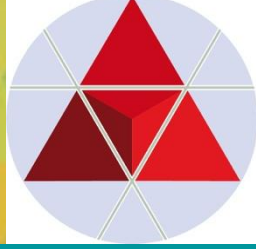
Source: Alexander Siedschlag, ZRK & ERAU, Vortrag IKT SIKON 2023

Methoden zur Störung von Satellitenkommunikation

- **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

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.

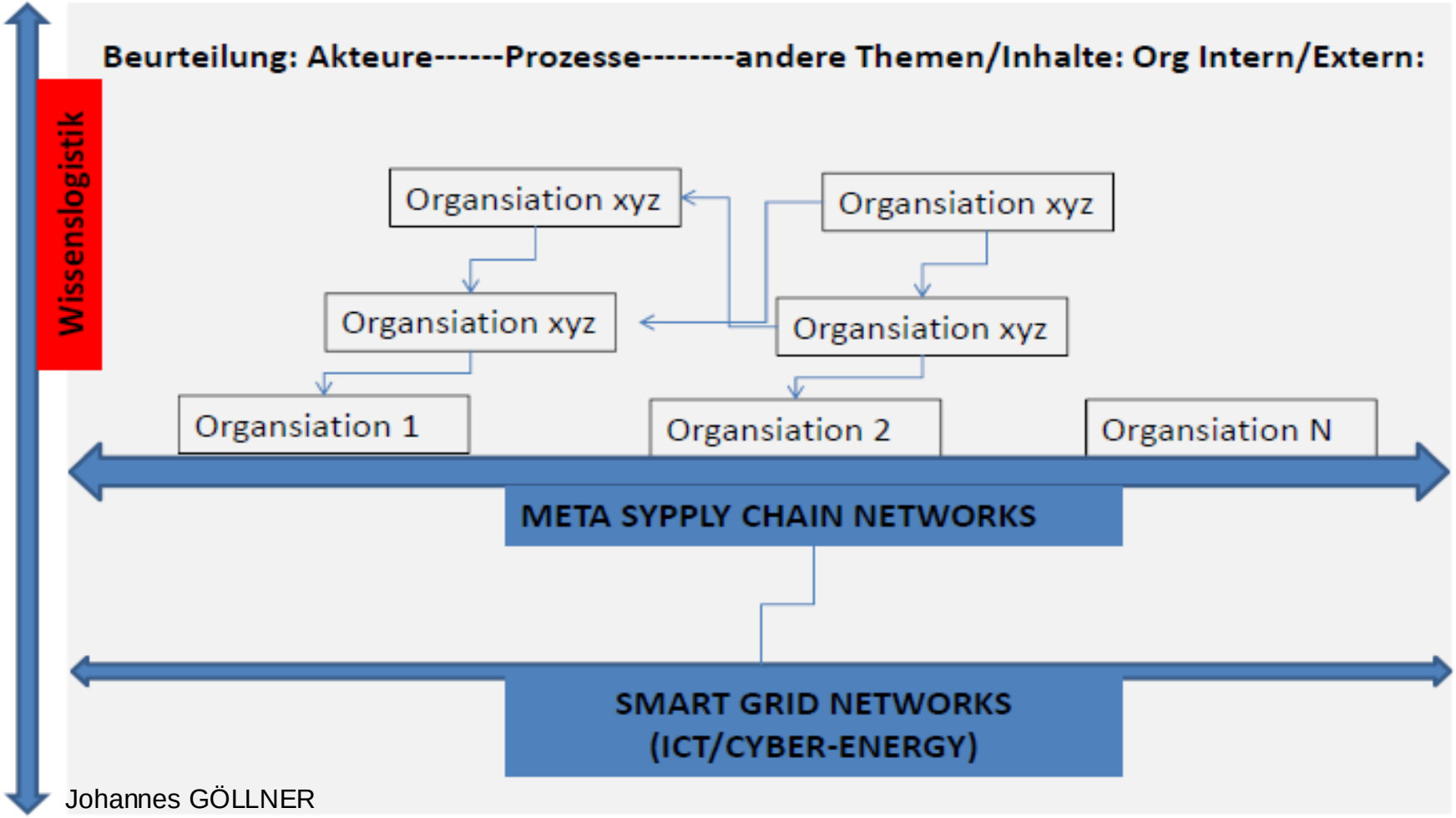
I. Basic Networks

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

III. Governmental & Public-/Administration Networks

Supply Chain Risk Management

KOMPLEXITÄT der Interaktionen/Vernetzungen

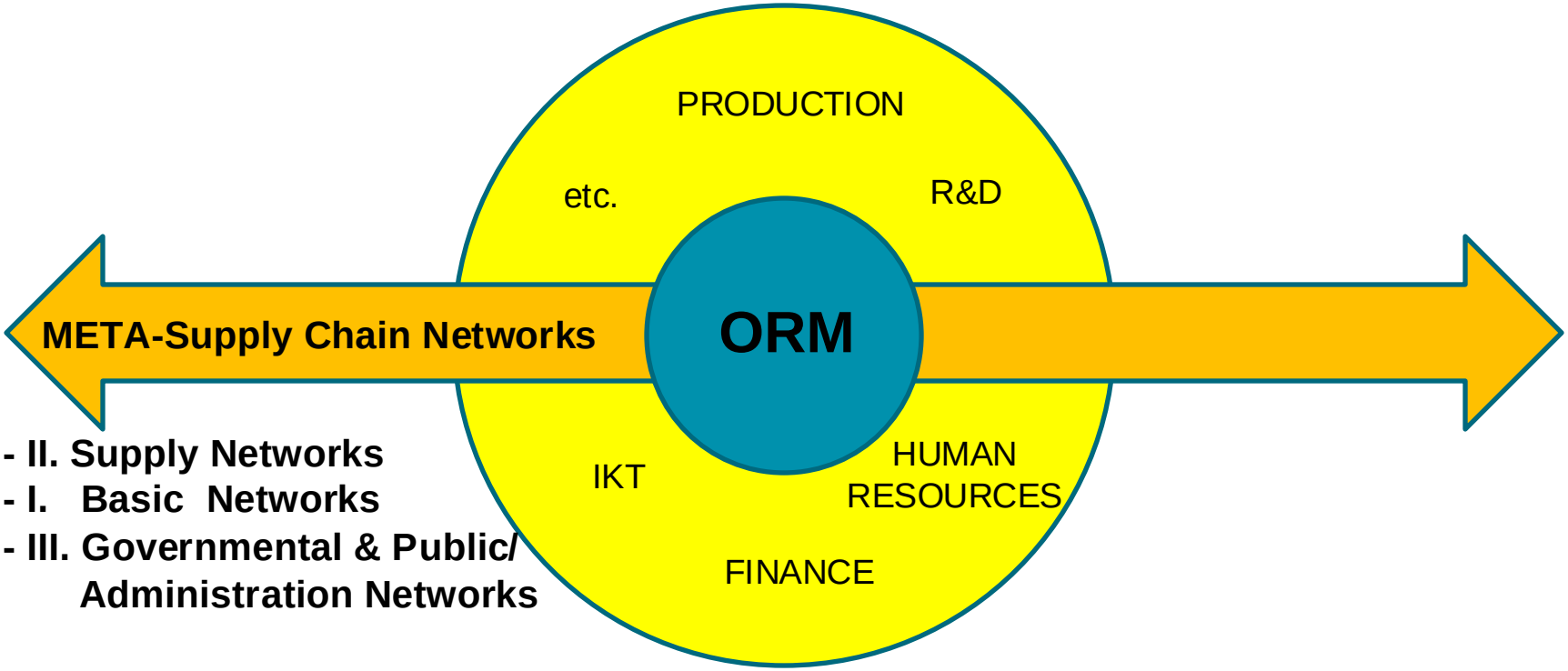


Johannes GÖLLNER

Source: Goellner Johannes, Qurichmayr Gerald: META-RISK: Meta-Risiko-Modell für kritische Infrastrukturen, *ICT-Security Conference 2016, St. Johann i./Pongau, Salzburg, Austria,12.10.2016*

Meta Supply Chain Model

Organisational Risk Management (ORM)

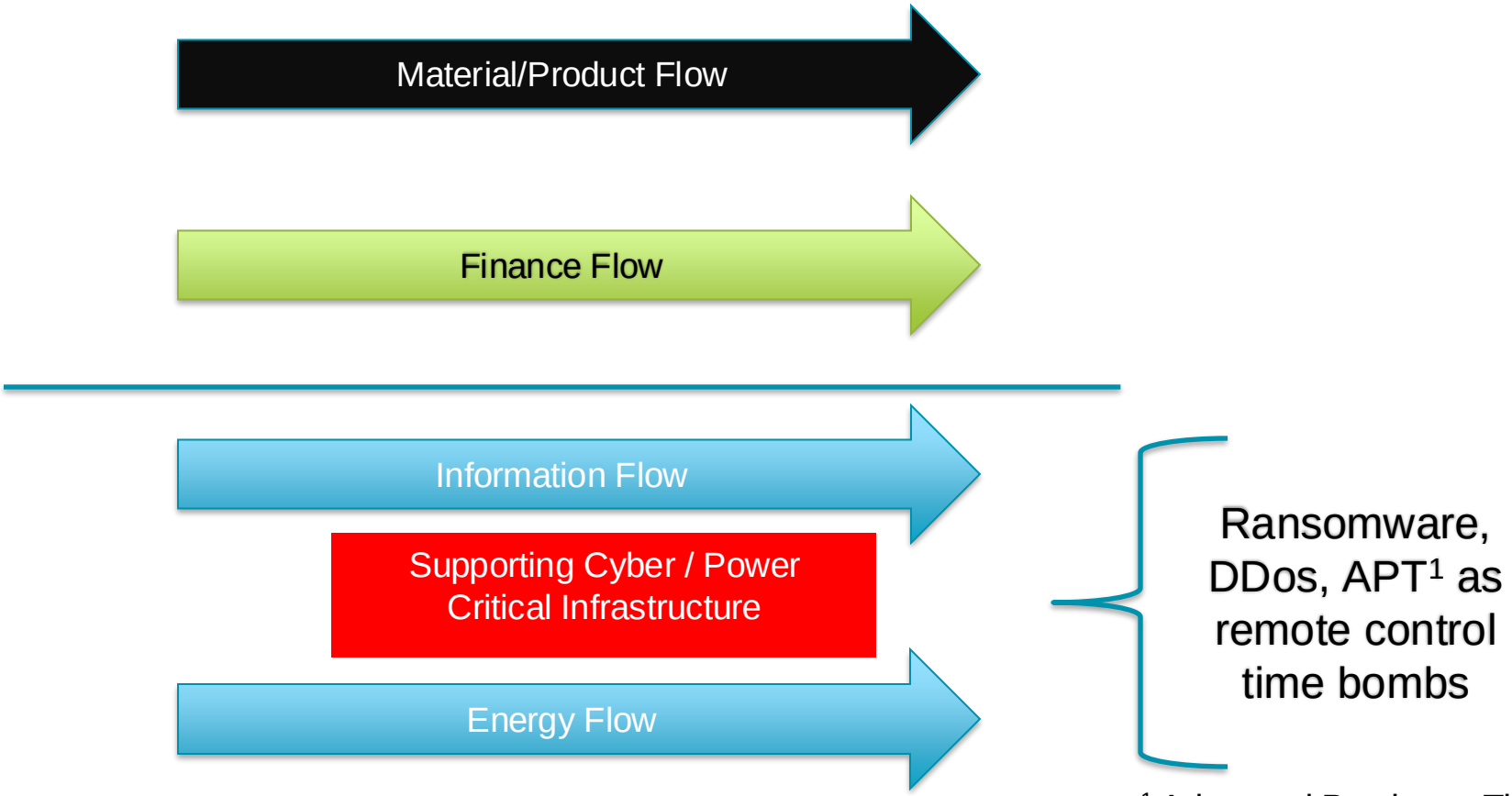


- **II. Supply Networks**
- **I. Basic Networks**
- **III. Governmental & Public/ Administration Networks**

relation: Organisation – Supply Chain Networks – ORM, Johannes Goellner

Enterprise Risks:

SCN Attack Points



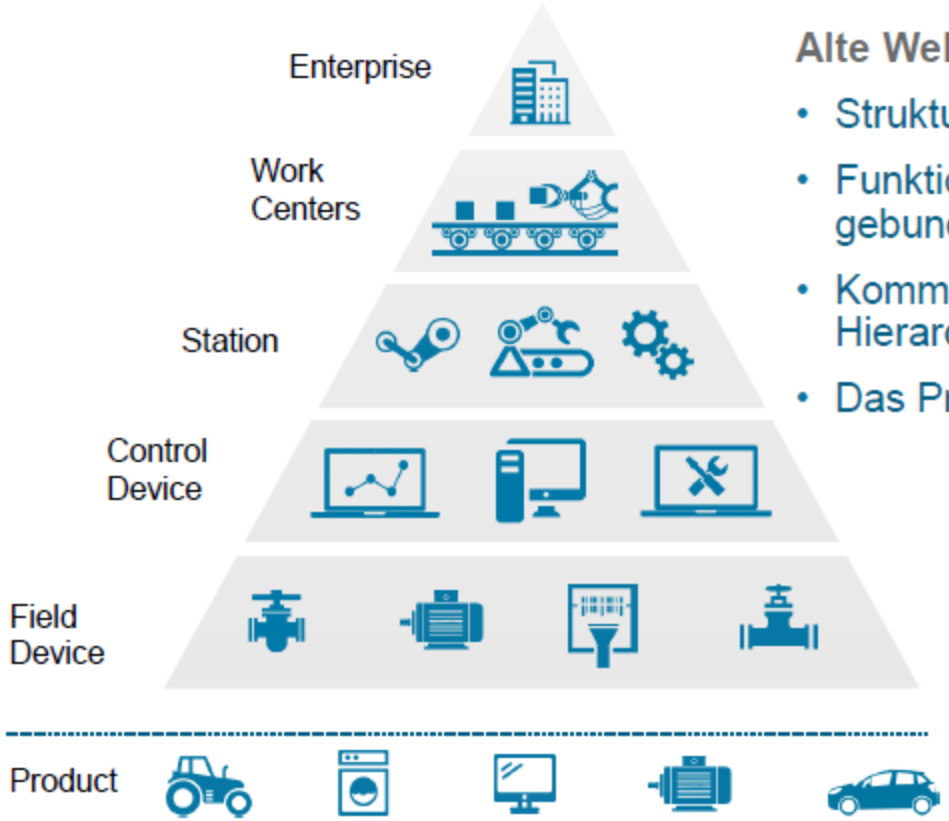
[1] Advanced Persistent Threat

Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

KOMPEXITÄT für IKT in der Supply Chain

PLATTFORM INDUSTRIE 4.0

Achse 1 – Hierarchie – Die Fabrik



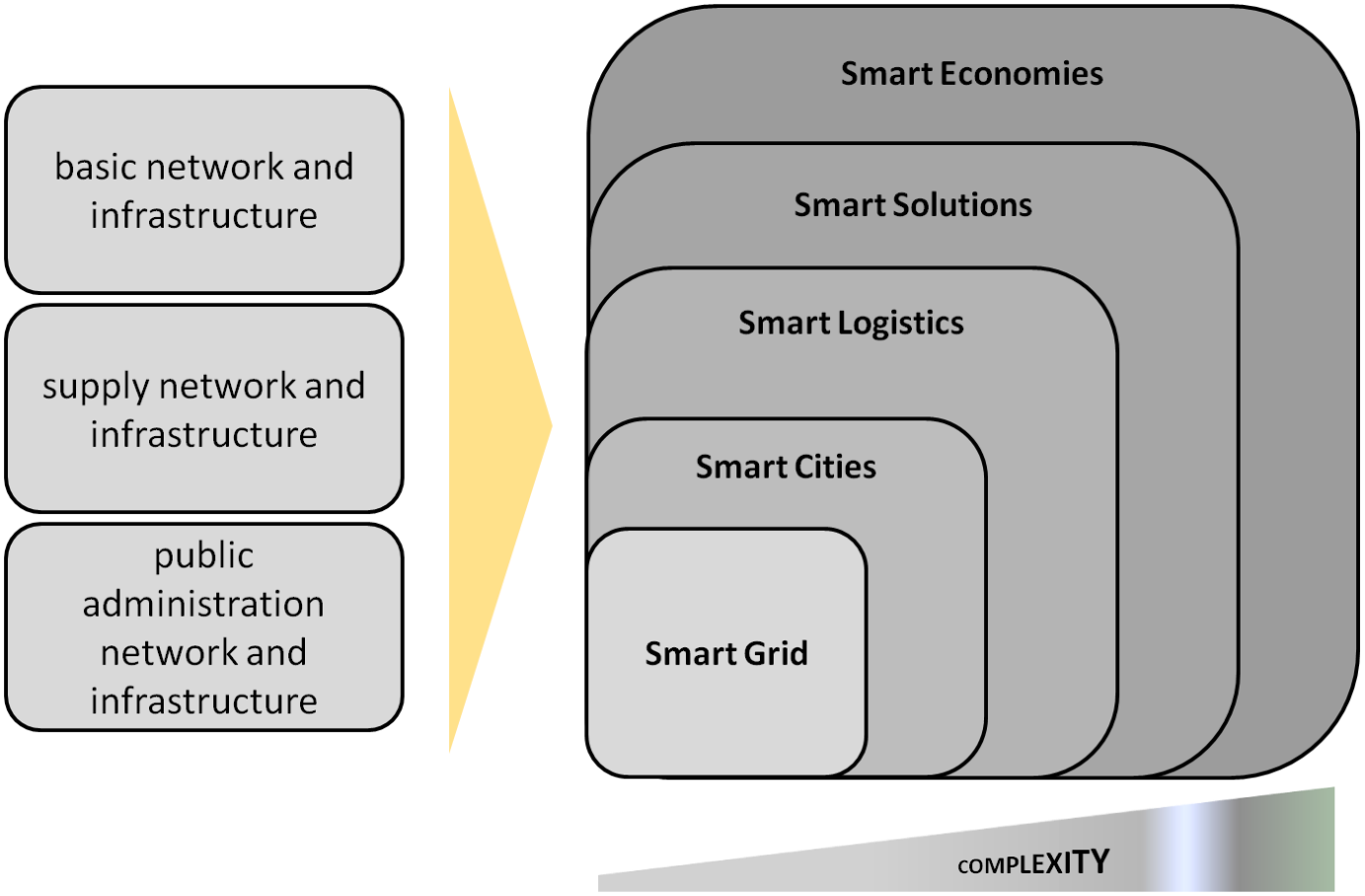
Alte Welt - Industrie 3.0

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

Supply Chain Risk- & Value Management

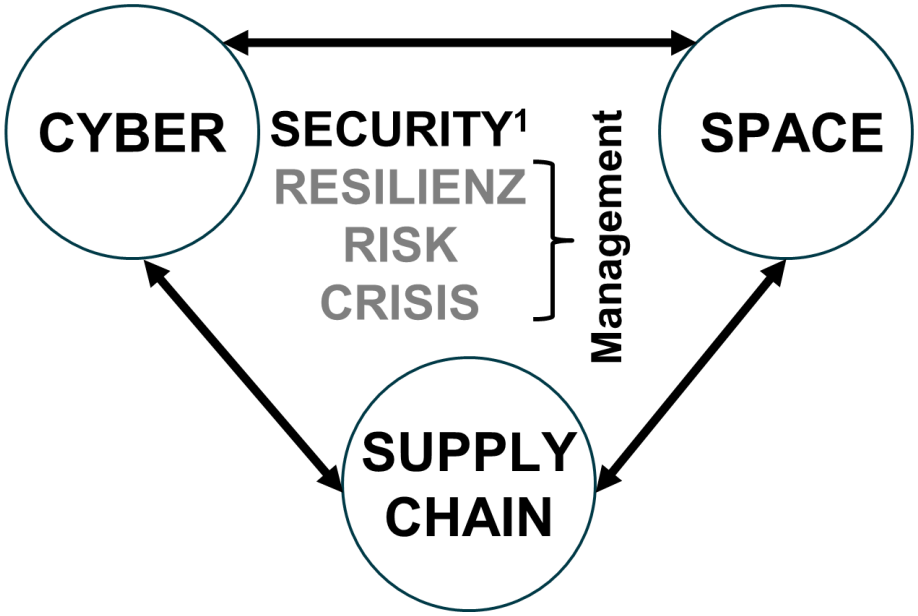
- *Supply Chain Resilience - Anforderungen*

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:

- Ernergie
- 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

EU CSDDD-Corporate Sustainability Due Diligence Directive

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937 of the European Parliament and of the Council of 15. March 2024

1. Einbeziehung der Sorgfaltspflicht in die Unternehmenspolitik
2. Ermittlung tatsächlicher und potenzieller negativer Auswirkungen
3. Vermeidung potenzieller negativer Auswirkungen
4. Behebung tatsächlicher negativer Auswirkungen
5. Beschwerdeverfahren

United Nations Global Compact (UNO, 2000)

DIE ZEHN PRINZIPIEN DES GLOBAL COMPACT

1. Unternehmen sollen den Schutz der internationalen **Menschenrechte** unterstützen und achten.
2. Unternehmen sollen sicherstellen, dass sie sich nicht an **Menschenrechtsverletzungen** mitschuldig machen.
3. Unternehmen sollen die **Vereinigungsfreiheit** und die wirksame Anerkennung des Rechts auf Kollektivverhandlungen wahren.
4. Unternehmen sollen für die Beseitigung aller Formen von **Zwangsarbeit** eintreten.
5. Unternehmen sollen für die Abschaffung von **Kinderarbeit** eintreten.
6. Unternehmen sollen für die Beseitigung von **Diskriminierung** bei Anstellung und Erwerbstätigkeit eintreten.
7. Unternehmen sollen im Umgang mit **Umweltproblemen** dem Vorsorgeprinzip folgen.
8. Unternehmen sollen Initiativen ergreifen, um größeres **Umweltbewusstsein** zu fördern.
9. Unternehmen sollen die Entwicklung und Verbreitung **umweltfreundlicher Technologien** beschleunigen.
10. Unternehmen sollen gegen alle Arten der **Korruption** eintreten, einschließlich Erpressung und Bestechung.

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

Risikomanagement:

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

Supply Chain Security Management:

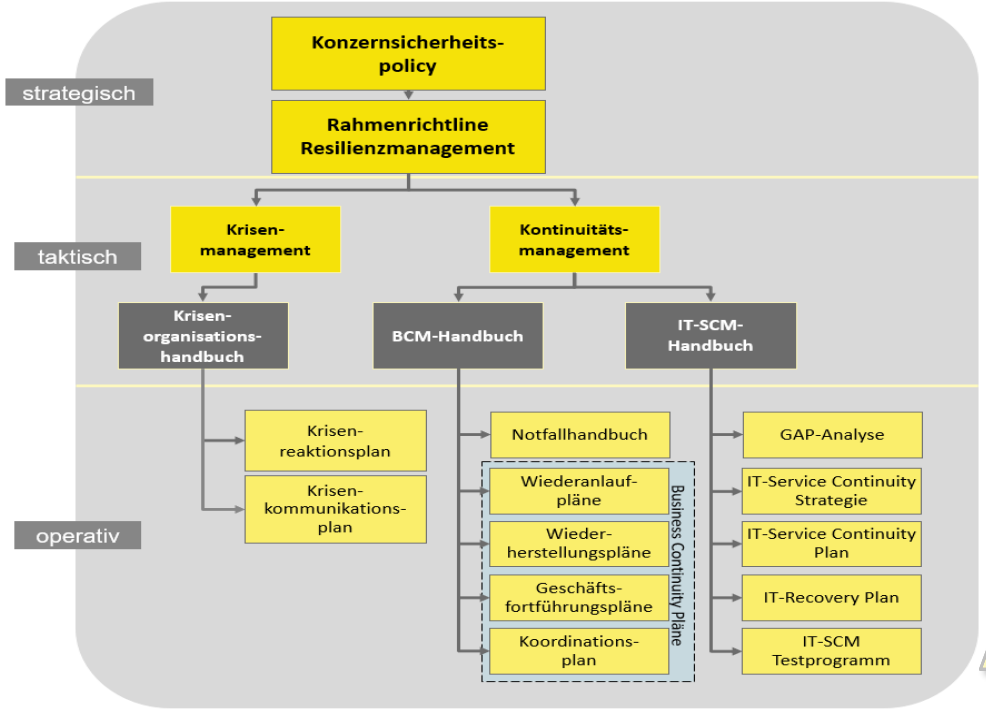
- ***ISO 28000*** *(Specification for security management systems for the supply chain), First edition: 2007-09-15; aktueller Stand: ISO 28000:2022; Revision in Vorbereitung.*
- ***ISO 28001*** *(Security management systems for the supply chain — Best practices for implementing supply chain security, 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;*

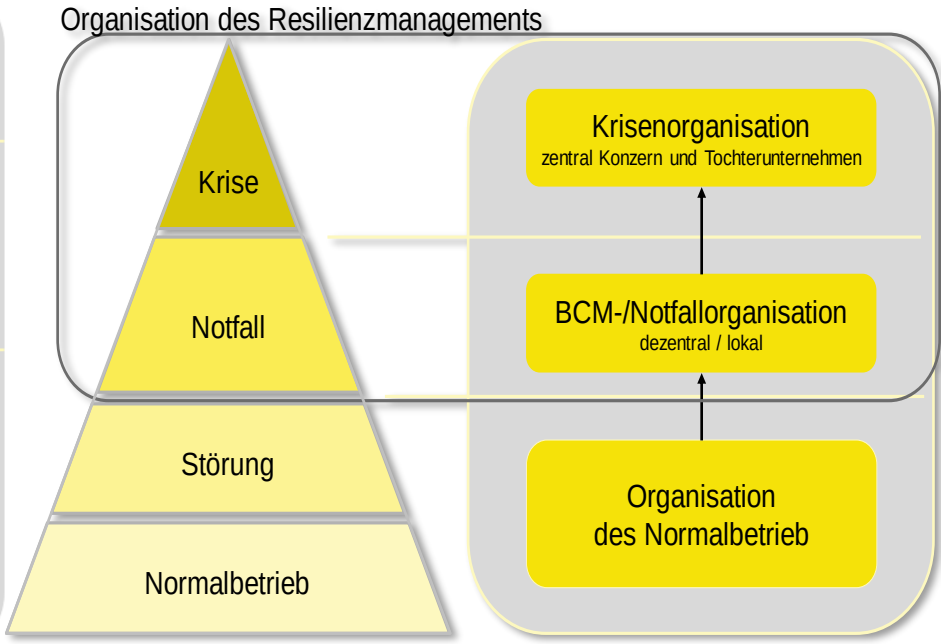
Krisenmanagement: vs. BCM *(vgl. NIS 2)*

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

„Krisenmanagement versus BCM“ im Rahmen eines RESILIENZMANAGEMENT

Implementierung **Resilienzmanagement**:



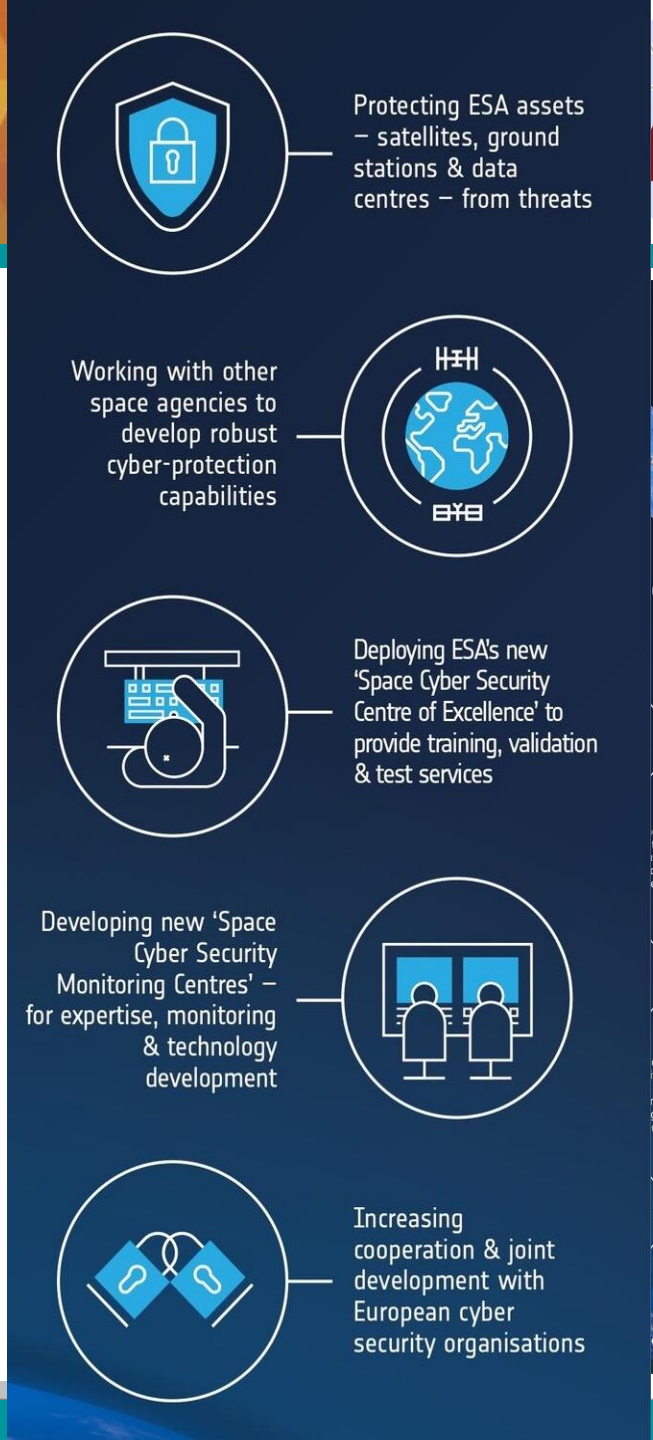


Quelle: Christian Paul, BSc MA, Post AG / IKT Sicherheitskonferenz 2023, 03.10.2023, 17:20, Linz, Österreich, link: ProgKonferenz.pdf (bundesheer.at)

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

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

LEITFÄDEN: *(intern./national), z.B.:*

- Leitfaden für Supply Chain Risk Management
  (Risk Management & Rating Association-RMA e.V., Stand 2015)
  - Link 1: Supply Chain Risk Management: RMA Risk Management & Rating Association (rma-ev.org)
- expected: Leitfaden für Supply Chain Resilience Management
  (Risk Management & Rating Association-RMA e.V., expected Ende Juni 2024!)

PUBLIKATIONEN:

- Risky Business:What Supply Chain Disruptions Really Cost, Everstream Analytics, 02.02.2022
  - Link 1: Special Reports - Everstream AI
  - ZRK-POSITIONSPAPIER: NIS 2 DIRECTIVE – ZRK – Zentrum für Risiko- und Krisenmanagement (zfrk.org)
- HANDBOOK OF CYBER DEVELOPMENT, CYBER DEMOCRACY, AND CYBER DEFENSE, Springer International Publishing, 2018
  - Global Supply Chain Network Risk Analysis and Monitoring for Global Cyber-Defense | SpringerLink
  - Bücher – ZRK – Zentrum für Risiko- und Krisenmanagement (zfrk.org)

Source: Johannes GÖLLNER, 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

The NIS 2 Directive

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022; *veröffentlicht im Europäischen Amtsblatt: 27.12.2022*)

„Bis 17.10.2024 erlassen und veröffentlichen die Mitgliedschaften die erforderlichen Vorschriften, um dieser Richtlinie nachzukommen. *Sie setzen die Kommission unverzüglich davon in Kenntnis.*

Die Mitgliedstaaten wenden diese Vorschriften ab dem 18.10.2024 an (vgl. Artikel 41 NIS-2 Richtlinie).

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 → "sichere Systemkonfiguration" (system hardening) ← Bewältigungsmaßnahmen

- 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

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

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.

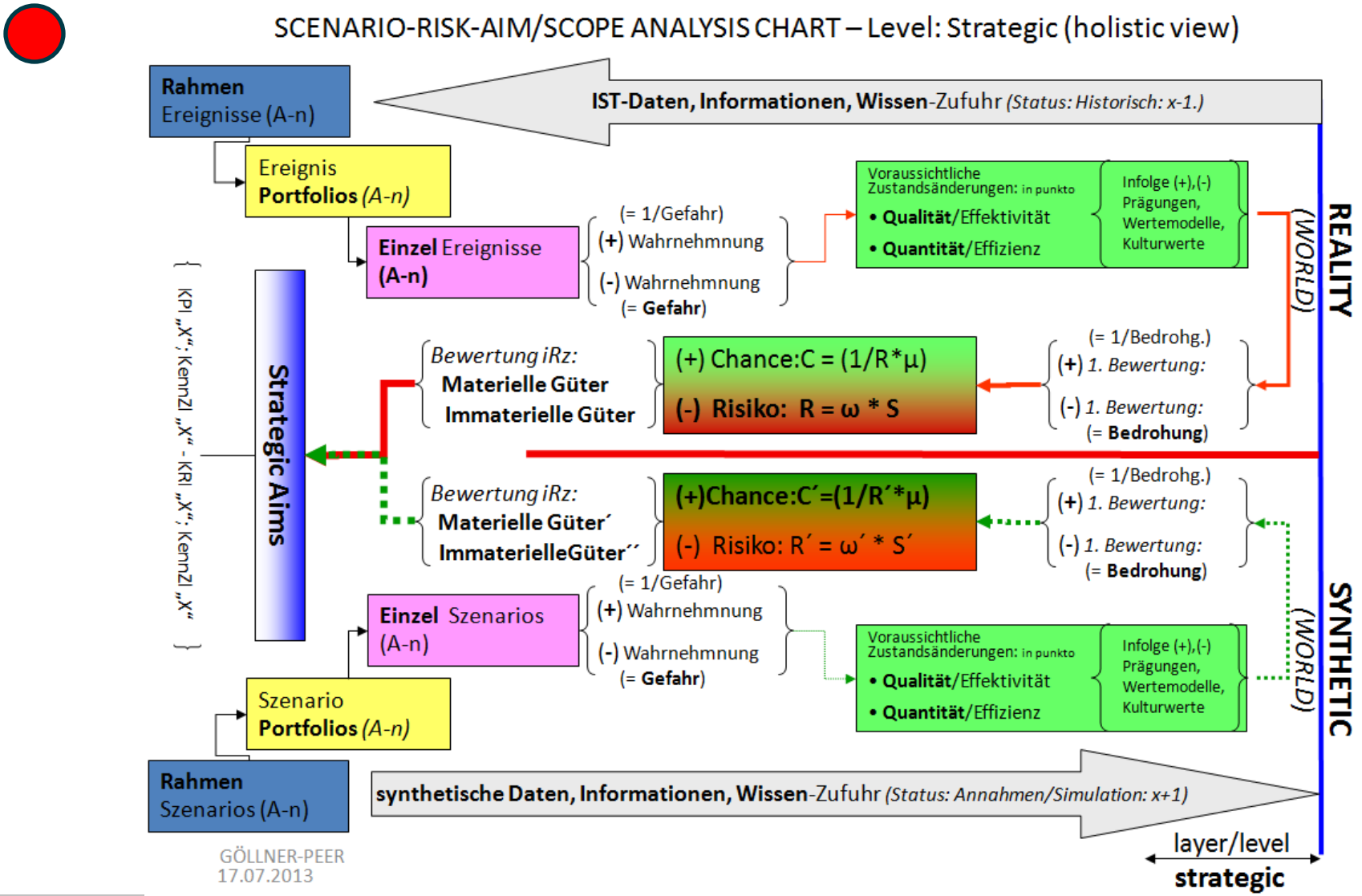
Geldbußen (Art 34): (bei Verstoß gegen Art 21 & Art 23)

- **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

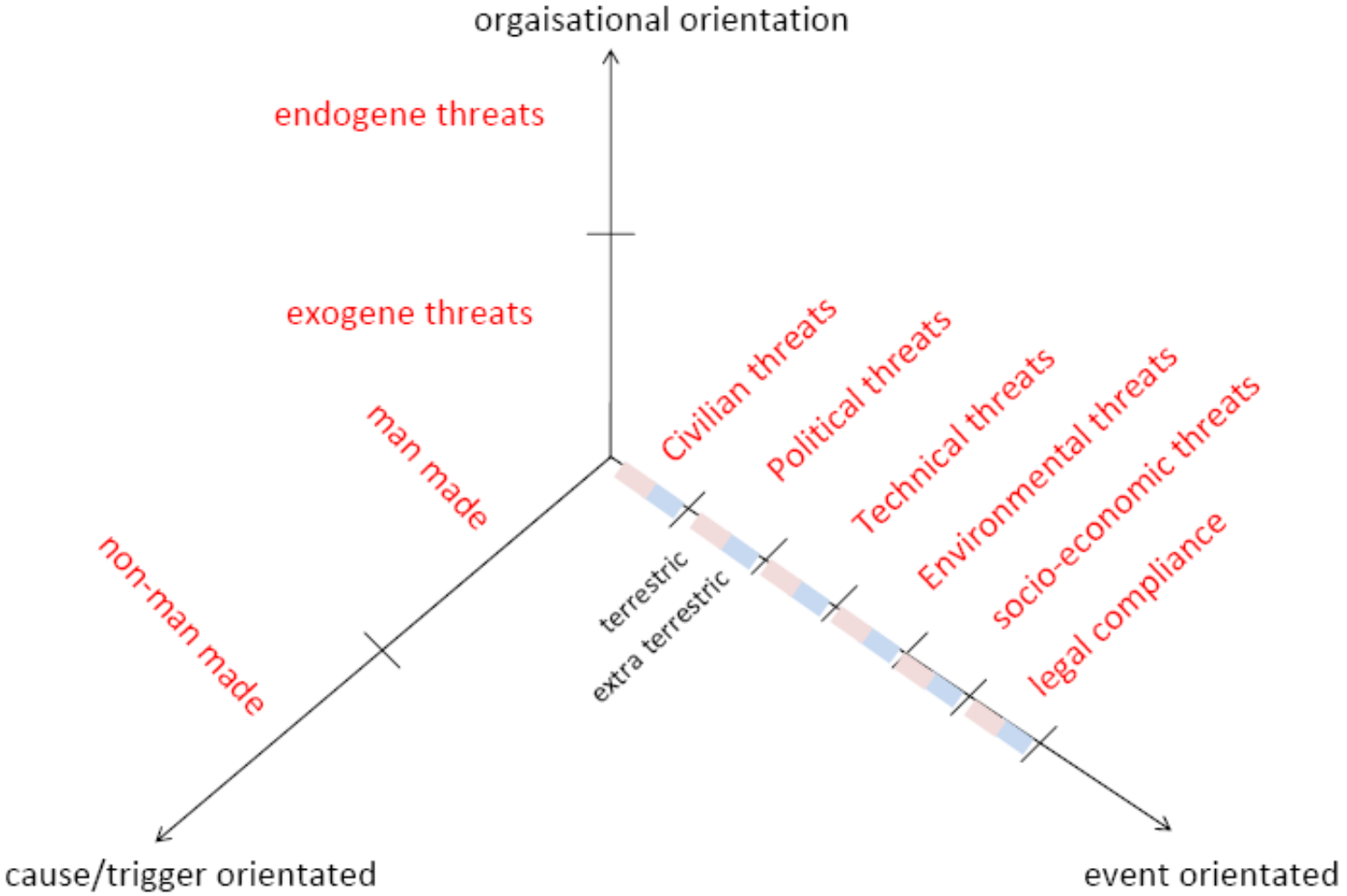
RISK MODELING
&
PERFORMANCE MONITORING SYSTEM

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



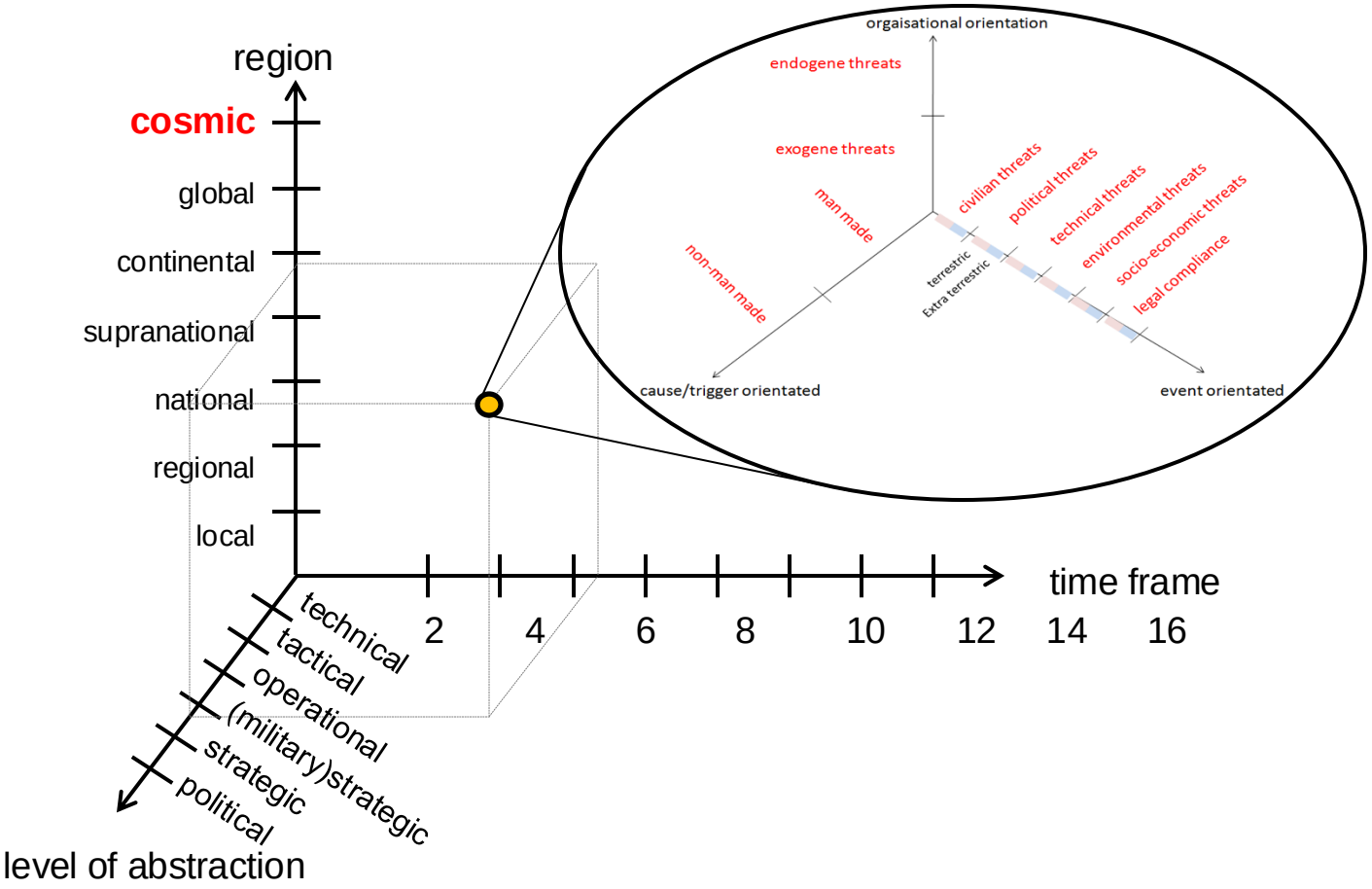
Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

Meta Model of an Organisation



Source: Johannes GÖLLNER, Vortrag IKT SIKON 2023

Multilayer Vector Model - Basis for Decision Making



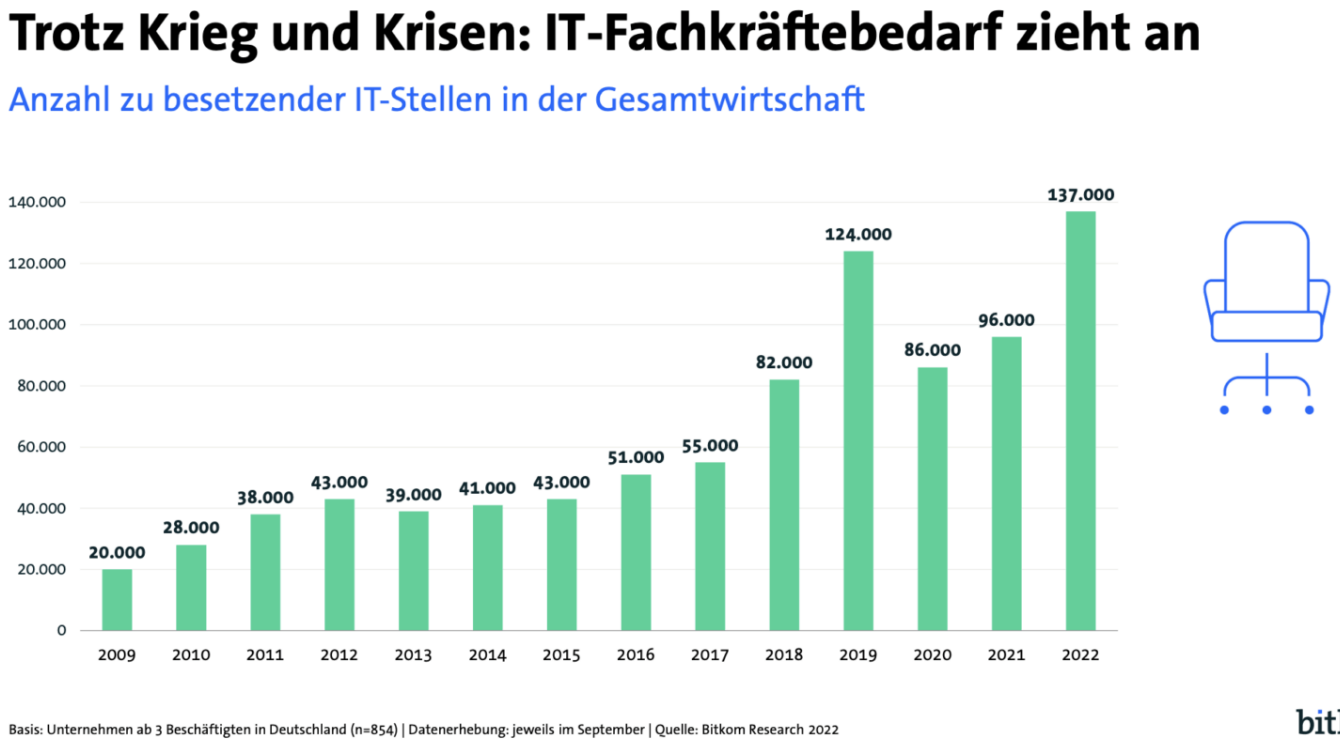
Quelle: Copyright by Zentraldokumentation/ Landesverteidigungsakademie, Wien, 12/2010 und 10/2011 (GÖLLNER, MAK, PEER, POVODEN)

BILDUNG

BILDUNG_Situation 1.1: Branche: Informations- und Kommunikationstechnik (IKT): DEUTSCHLAND

Bitkom-Studie: 137.000 IT-Vakanzen in 2022:

In der folgenden Grafik der neusten Bitkom-Studie zum IT-Fachkräftemangel vom **16. November 2022**, können Sie sehen, wie sich die Anzahl an offenen Stellen in der IT in den letzten Jahren entwickelt hat:



BILDUNG_Situation 1.2: Branche: Informations- und Kommunikationstechnik (IKT): DEUTSCHLAND

Studie von McKinsey & Company zum IT-Fachkräftemangel im Öffentlichen Dienst:

Laut einer am 25.01.2023 veröffentlichten Studie der Unternehmensberatung McKinsey & Company, benötigt der öffentliche Dienst bis 2030 insgesamt **840.000 Vollzeitfachkräfte**, wobei die Personallücke in den IT- und Digitalberufen besonders groß sei.

Bei Bund, Ländern und Kommunen würden bereits heute rund 39.000 Fachkräfte in Informatik- und IT-Berufen fehlen. Bis 2030 würden es rund 140.000 IT-Fachkräfte sein.

BILDUNG_Situation 2: Branche: Informations- und Kommunikationstechnik (IKT): ÖSTERREICH

- Fachkräfte bereits vor dem Ausbruch der Pandemie rar gesät gewesen, mit dem Digitalisierungsschub durch Corona sei die Lücke aber noch größer geworden.

- Laut aktuellen Daten des Fachverbandes Unternehmensberatung und Informationstechnologie (Ubit) der Wirtschaftskammer **Österreich fehlen rund 24.000 IT-Fachkräfte in Österreich, was jährlich einen Wertschöpfungsverlust von 3,8 Milliarden Euro auslöse.**

- **In den kommenden fünf Jahren rechnet der Verband mit einer Lücke von rund 30.000 Fachleuten.** ***(2022-2027)***

Source: Alfred Harl, Obmann des Fachverbands Unternehmensberatung und Informationstechnologie (Ubit) in der Wirtschaftskammer, bei einem Online-Pressegespräch, Quelle: https://www.nachrichten.at/wirtschaft/it-branche-schlaegt-alarm-30000-fachleute-fehlen;art15,3584306

Ideenbeitrage/Lösungsoptionen:

Anm: Fachleute aus Drittstaaten nach DE und AT einfacher zu machen ?

1. **Schaffung von mehr Studien- und Ausbildungsplätzen** an
    1. **DE:** Gymnasium und Fachoberschule
    2. **AT:** Allgemein Bildenden & Höheren Berufsbildenden Mittelschulen (HAK & HTBLA)
    3. Facheinschlägigen Fachhochschulen
    4. Facheinschlägigen öffentlich-rechtlichen und privatrechtlichen Universitäten

2. Im Sinne der **benötigten REIFEGRADE** des erforderlichen **HC-Human Capital**: (in punkto: 5 Kompetenzfelder !!)
    1. **Reifegrade 1-10:** (EQR-Def. Level 6 & 7, mit beruflicher Expertise))
    2. **Dublin Deskriptoren** (1-5) beachten!
        - (Noten: sind ein Problem, weil Sie nicht das **theoretische Können abbilden!!)**
3. **Ethische Verortung!?!**

Source: Johannes GÖLLNER & Prof. DDr. Martin STIEGER, Vortrag IKT SIKON 2023

Fazit: aus unserer Sicht !!

1. **Wenn es so ist, ..:**

- dann sind die Unternehmen in der Aus-, Fort-, und Weiterbildung unersetzlich und daher in der Eigenverantwortung (Beispiel: Corporate Universities, siehe in den 1980-1999, Motorola, SAP, KLU,…, McDonald)

- **Annahme: Vorteil ist:** kein Unternehmen möchte grundsätzlich seine Mitbewerber ausbilden!

- **Haben wir überhaupt die geeigneten und höchst qualifizierten Lehr- und Ausbildungskräfte!!!!** (Entlohnung, Vergütungsformen,…)

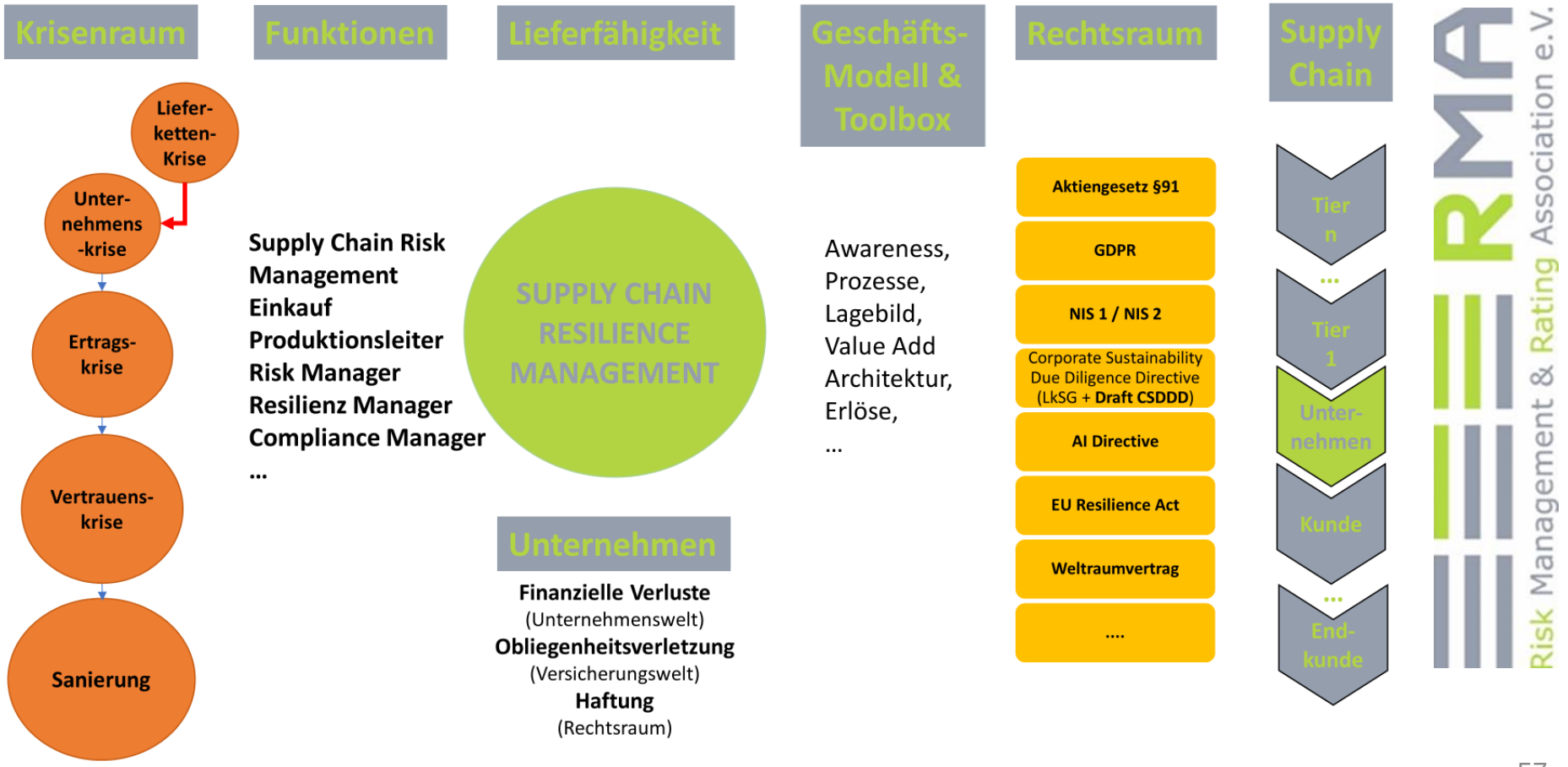
- etc.

RMA-LEITFADEN:

„Supply Chain Resilience Management“

Lösungsansätze: Beitrag RMA e.V., AK SCRM

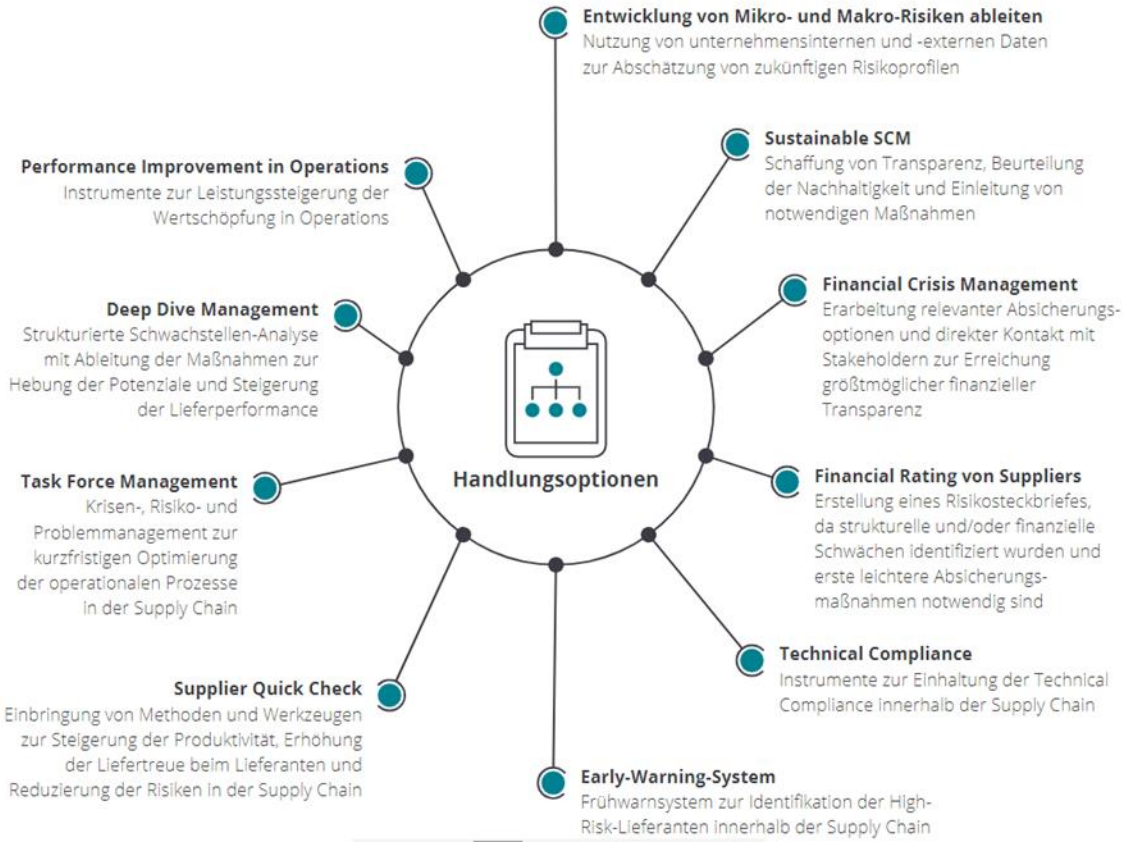
RMA-Leitfaden: SUPPLY CHAIN RESILIENZ MANAGEMENT



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: 06/2024 (expected)
SUPPLY CHAIN RESILIENZ MANAGEMENT



Source: Deloitte, 2023

SUPPLY CHAIN ANALYSE (z.B. für KMU)

nachfolgend der Link zum kostenfreien Supply Chain Quick Check von der FUNK-Stiftung:

https://supplychain.risk-quickcheck.de/de/

und weitere Informationen und eine Videoeinführung zur Handhabung:
https://www.funk-stiftung.org/de/risikomanagement/projekte/risk-assessment-tool-quick-check

RMA-Partner & Sponsor

VI. FAZIT & AUSBLICK I:

Im Nachfolgenden sind einige Herausforderungen angeführt, welche für NIS 2-betroffene Unternehmen – *und im besonderen KMU* – relevant sind:

1. *Entwicklung und Anwendung eines standardisierten, fakten- und auf einem mathematischen modellbasierten Cyber-Event und Bedrohungs-Monitoring sowie eines Risikoanalyse- und -bewertung-Modelles, sowie der notwendigen – teils permanenten – Dokumentation der Zusammenhänge und Wechselwirkungen, basierend auf den aktuell relevanten gesetzlichen Innovationen zwischen Space-, Cyber- und Supply Chain-Regelwerken.*
2. *Die Anforderungen und Strategische Ansätze: Status Quo und Innovationen für die Risikomodellierung & -monitoring in Bezug auf Zertifizierungen, Audits und Bonitätsprüfungen im Rahmen einer M&A-Due Diligence werden die Unternehmen (Einrichtungen) vor große Herausforderungen stellen, um Vertrauen bei bzw. in den betroffenen Unternehmen, Investoren und den nationalen zuständigen Aufsichtsbehörden zu begründen, und um eine reduzierte Innovationsfreude -besonders bei KMU- oder Druck auf die digitale Transformation der KMU zu vermeiden.*
3. *Die Verfügbarkeit von qualitätsgesicherten modellbasierten Cyber-/Lieferketten Event und Bedrohungs-Monitoring-, Risikoanalyse- und Risikobewertungs-Werkzeugen sind fachlich eingeschränkt.*

VI. FAZIT & AUSBLICK II:

4. Die Mitentwicklung von Leitfäden und einheitlichen qualitätsgesicherten und getesteten Zertifizierungsstandards ist relevant, um die entstehenden Kosten *(wie z. B. infolge zusätzlicher Überwachung, zusätzlicher -womöglich permanenter- Berichterstattung von Vorfällen und Bedrohungen, Supply Chain Security, zusätzlicher Vollzugskosten, einschließlich des zusätzlichen Rahmens für das Krisenmanagement, etc.)* bei der Erfüllung der NIS 2-Richtlinie Vorgaben reduzieren zu können.
5. Initiierung einer Aus-, Fort- und Weiterbildung-Kampagne zur Bewältigung des existierenden facheinschlägigen IT/Cyber-Fachkräftemangels bei österreichischen Unternehmen sowie der Ausbildung aktuell in Österreich nicht in der entsprechenden Anzahl verfügbaren NIS 2-Zertifizierungsexperten, um die nach ISO 27001, etc. in großer Anzahl zu erwartenden zu auditierenden Unternehmen fachlich und zeitnah bedienen zu können.
6. Derzeit existiert noch kein verfügbares, inhaltlich qualitätsgesichertes Top-Management-Ausbildungskonzept für die die Zielgruppe: Top-Management (Geschäftsführer, Vorstände, Aufsichtsräte, Beiräte, etc.) im Sinne der Verantwortlichkeit des Top-Managements, gemäß NIS 2-Richtlinie.

Globale Chancen: ZRK-INITIATIVE

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!
17.09.2024, im Rahmen der IKT-Sicherheitskonferenz in Wien !

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 Fähgikeit zur Verteidigung nationaler Interessen, Wachstumssektor Weltraumwirtschaft, erhöhte internationale Glaubwürdigkeit

Pfeiler weltraumpolitischer Sicherheitsarchitektur

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 Erdbeobachtungsfähigkeiten zur Resilienzbildung im Rahmen von Katastrophenmanagement
- Förderung der Kompatibilität, Interoperabilität und Transparenz zwischen satellitengestützten Informationssystemen
- Nutzung des Weltraums die Sustainable Development Goals (SDG)
- Long-Term Sustainability (LTS) of Outer Space Activities (Weltraumrecht; Betriebssicherheit von Weltraumoperationen; internationale Zusammenarbeit in der Fähigkeitenentwicklung; Bewusstseinsbildung)

- **Internationale Organisation**
- Cybersecurity-Initiative:
  - ❑ Relevante Aktivitäten konsolidieren (threat monitoring, cyber defence, education, etc.)
  - ❑ Technologieentwicklung einbeziehen: Quantum cryptography, optical communication
  - ❑ Kosteneffiziente Implementierung von Sicherheitsmechanismen durch Standardisierung (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 Satellitennavigationssystem 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

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

Kontakte

Johannes L. GOELLNER

Leiter RMA-AK-SCRM &
(Vorstandsmitglied RMA e.V.)
www.rma-ev.org, München
email: johannes.goellner@rma-ev.org
mobil: +[43]-650-2252991

Vizepräsident der Verwaltung
Genossenschaft für Digitalisierung,
Challenge & Innovationsmanagement
www.gdcim.coop , Volketswil/Zürich

Vorstandsvorsitzender *des*
Zentrum für Risiko- und
Krisenmanagement,Wien
und des
Internationalen CYBER-Hilfswerk, Zürich
www.zfrk.org & www.cyber-hw.org
email: johannes.goellner@zfrk.org

Ralf A. HUBER

Vorstandsmitglied RMA e.V. &
Mitglied des RMA-AK-SCRM
www.rma-ev.org, München
email: ralf.huber@rma-ev.org
mobil: +[49]-163-9809054

Stiftungsratsmitglied
Funk Stiftung

www.funk-stiftung.org , Hamburg

Compliance & Risk Management
STAEDTLER SE

www.staedler.com , Nürrnberg
email: ralf.huber@staedtler.com

RMA
Risk Management & Rating Association e.V.

Zentrum für
Risiko- & Krisenmanagement

Thank you for your attention.

excellent.
connected.
individual.