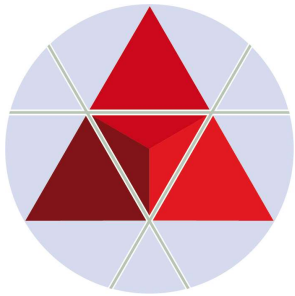
IKT SIKON 2023

Linz, 03.10.2023, 10:30-10:50 Uhr



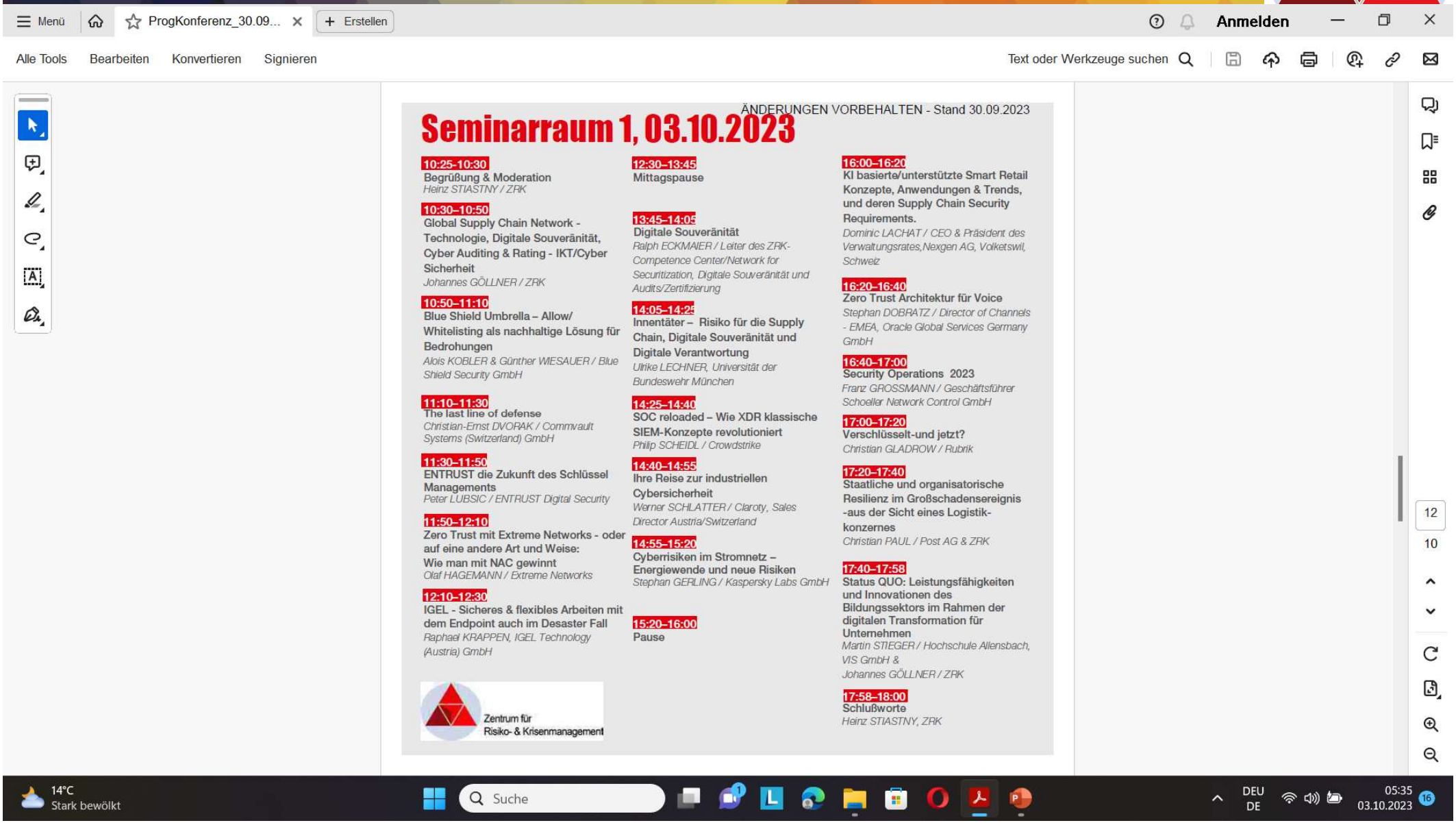
Zentrum für
Risiko- & Krisenmanagement

Global Supply Chain Netzwork - Technologie, Digitale Souveränität, Cyber Auditing & Rating-ICT/Cyber Sicherheit

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

excellent.
connected.
individual.

I. Überblick:



ÄNDERUNGEN VORBEHALTEN - Stand 30.09.2023

Seminarraum 1, 03.10.2023

10:25-10:30
Begrüßung & Moderation
Heinz STIASTNY / ZRK

10:30–10:50
Global Supply Chain Network - Technologie, Digitale Souveränität, Cyber Auditing & Rating - IKT/Cyber Sicherheit
Johannes GÖLLNER / ZRK

10:50–11:10
Blue Shield Umbrella – Allow/ Whitelisting als nachhaltige Lösung für Bedrohungen
Alois KOBLER & Günther WIESAUER / Blue Shield Security GmbH

11:10–11:30
The last line of defense
Christian-Ernst DVORAK / Commvault Systems (Switzerland) GmbH

11:30–11:50
ENTRUST die Zukunft des Schlüssel Managements
Peter LUBSIC / ENTRUST Digital Security

11:50–12:10
Zero Trust mit Extreme Networks - oder auf eine andere Art und Weise: Wie man mit NAC gewinnt
Olaf HAGEMANN / Extreme Networks

12:10–12:30
IGEL - Sicheres & flexibles Arbeiten mit dem Endpoint auch im Desaster Fall
Raphael KRAPPEN, IGEL Technology (Austria) GmbH

Zentrum für Risiko- & Krisenmanagement

12:30–13:45
Mittagspause

13:45–14:05
Digitale Souveränität
Ralph ECKMAIER / Leiter des ZRK-Competence Center/Network for Securitization, Digitale Souveränität und Audits/Zertifizierung

14:05–14:25
Innentäter – Risiko für die Supply Chain, Digitale Souveränität und Digitale Verantwortung
Ulrike LECHNER, Universität der Bundeswehr München

14:25–14:40
SOC reloaded – Wie XDR klassische SIEM-Konzepte revolutioniert
Philip SCHEIDL / Crowdstrike

14:40–14:55
Ihre Reise zur industriellen Cybersicherheit
Werner SCHLATTER / Claroty, Sales Director Austria/Switzerland

14:55–15:20
Cyberrisiken im Stromnetz – Energiewende und neue Risiken
Stephan GERLING / Kaspersky Labs GmbH

15:20–16:00
Pause

16:00–16:20
KI basierte/unterstützte Smart Retail Konzepte, Anwendungen & Trends, und deren Supply Chain Security Requirements.
Dominic LACHAT / CEO & Präsident des Verwaltungsrates,Nexgen AG, Volketswil, Schweiz

16:20–16:40
Zero Trust Architektur für Voice
Stephan DOBRATZ / Director of Channels - EMEA, Oracle Global Services Germany GmbH

16:40–17:00
Security Operations 2023
Franz GROSSMANN / Geschäftsführer Schoeller Network Control GmbH

17:00–17:20
Verschlüsselt-und jetzt?
Christian GLADROW / Rubrik

17:20–17:40
Staatliche und organisatorische Resilienz im Großschadensereignis -aus der Sicht eines Logistik-konzernes
Christian PAUL / Post AG & ZRK

17:40–17:58
Status QUO: Leistungsfähigkeiten und Innovationen des Bildungssektors im Rahmen der digitalen Transformation für Unternehmen
Martin STIEGER / Hochschule Allensbach, VIS GmbH &
Johannes GÖLLNER / ZRK

17:58–18:00
Schlußworte
Heinz STIASTNY, ZRK

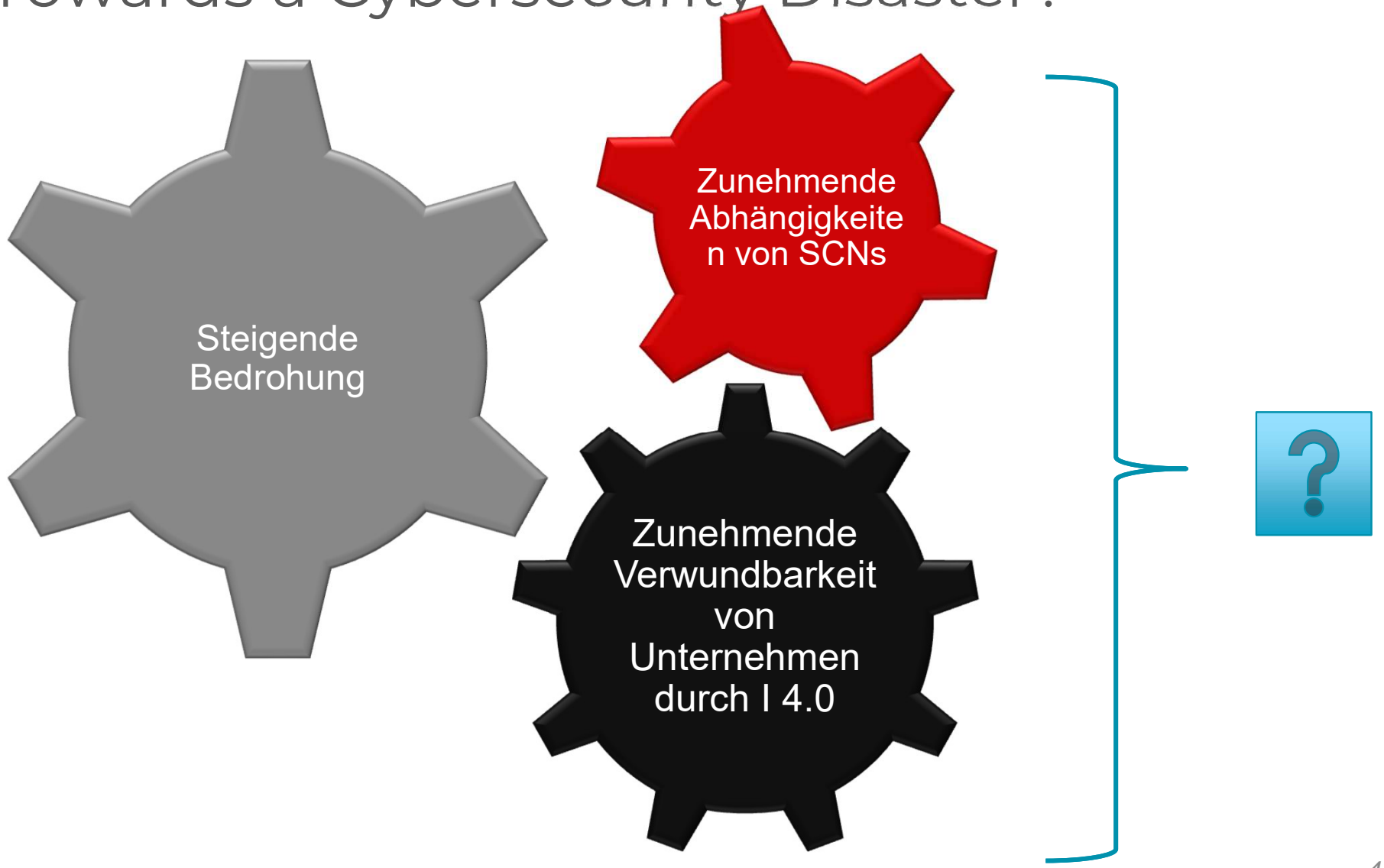
I. Überblick:

- Auszugsweise Darstellung und Diskussion der **Zusammenhänge-Wechselwirkungen der aktuell relevanten gesetzlichen Innovationen zwischen Cyber- und Supply Chain-Regelwerken.**

- **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.

- **Lösungsansätze: Regelwerke/Leitfäden**

Towards a Cybersecurity Disaster?



4

Überblick I.1: 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

I. Enterprise Risks:
Unterschätztes Risiko Supply Chain [Networks]:

Supply Chains -> : Networks of Supply Chains

- *Erhöhte Komplixität*
- *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

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

II. 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:

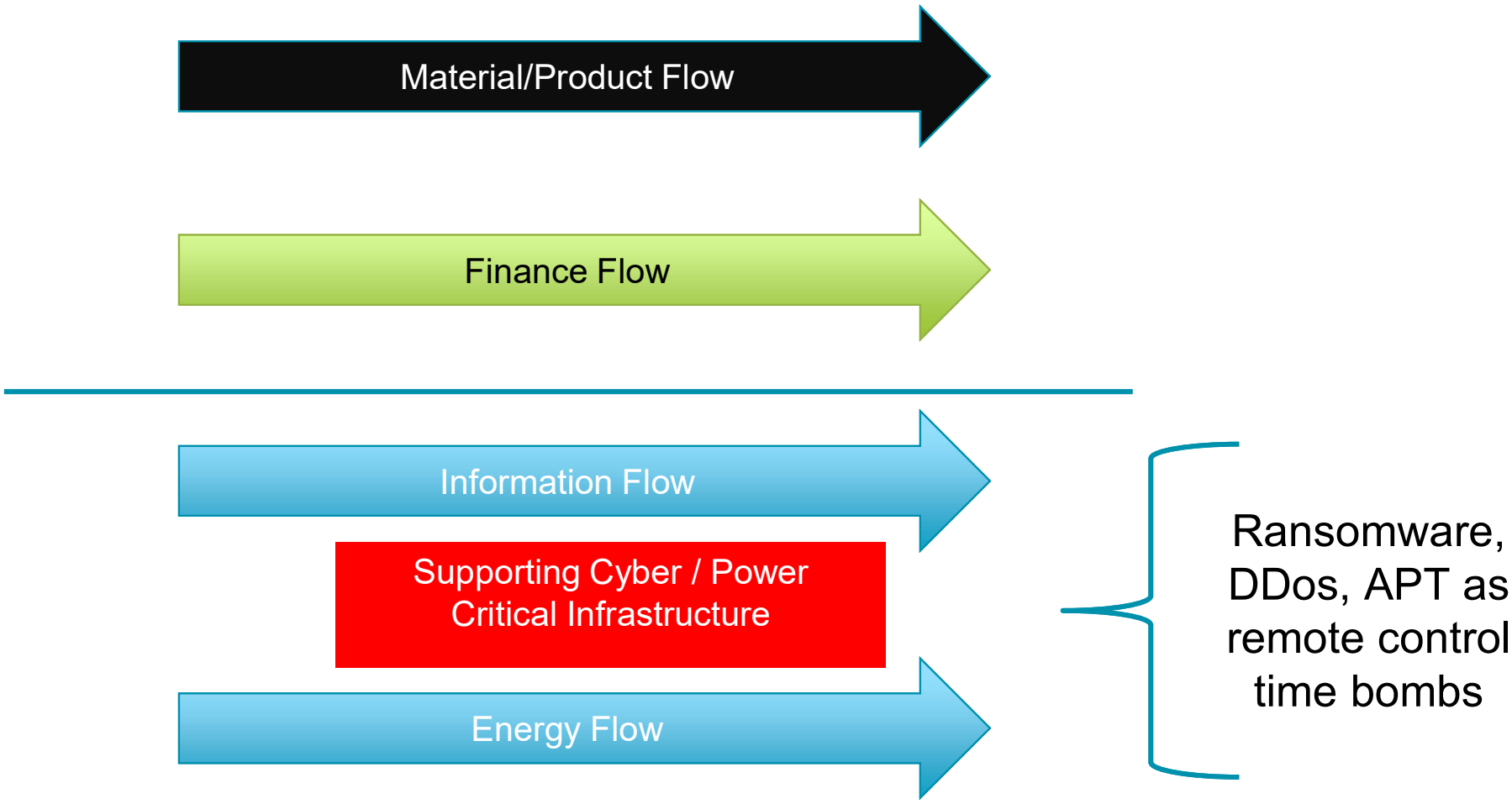
1. **Production stoppage or slowdown:** *Direct losses occur when production lines are forced to idle due to key components or inputs being unavailable. The daily cost of a halted production line is the most obvious cost but there may also be other related costs.*
2. **Higher freight costs:** *Inputs 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

I. Enterprise Risks:

SCN Attack Points



Cybercrime - ein wachsendes Problem

APT, WannaCry, Petya, ... (Europa 2017 and ongoing)
Insider-Datendiebstahl im Outsourcing (laufend)
Gestohlene und verlorene Datenträger (laufend)
Information Operations aka Information Warfare (laufend)
Organisierte Kriminalität, insb. Geldwäsche (laufend)
Angriffe auf Kritische Infrastrukturen (seit einigen Jahren – APT, Ransomware)

- *BIS-Betriebliche Informationssysteme:*
  - **ERP- und SCM-Systeme : Frage von massiven Angriffen ist nicht OB, sondern WANN?**

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.

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.

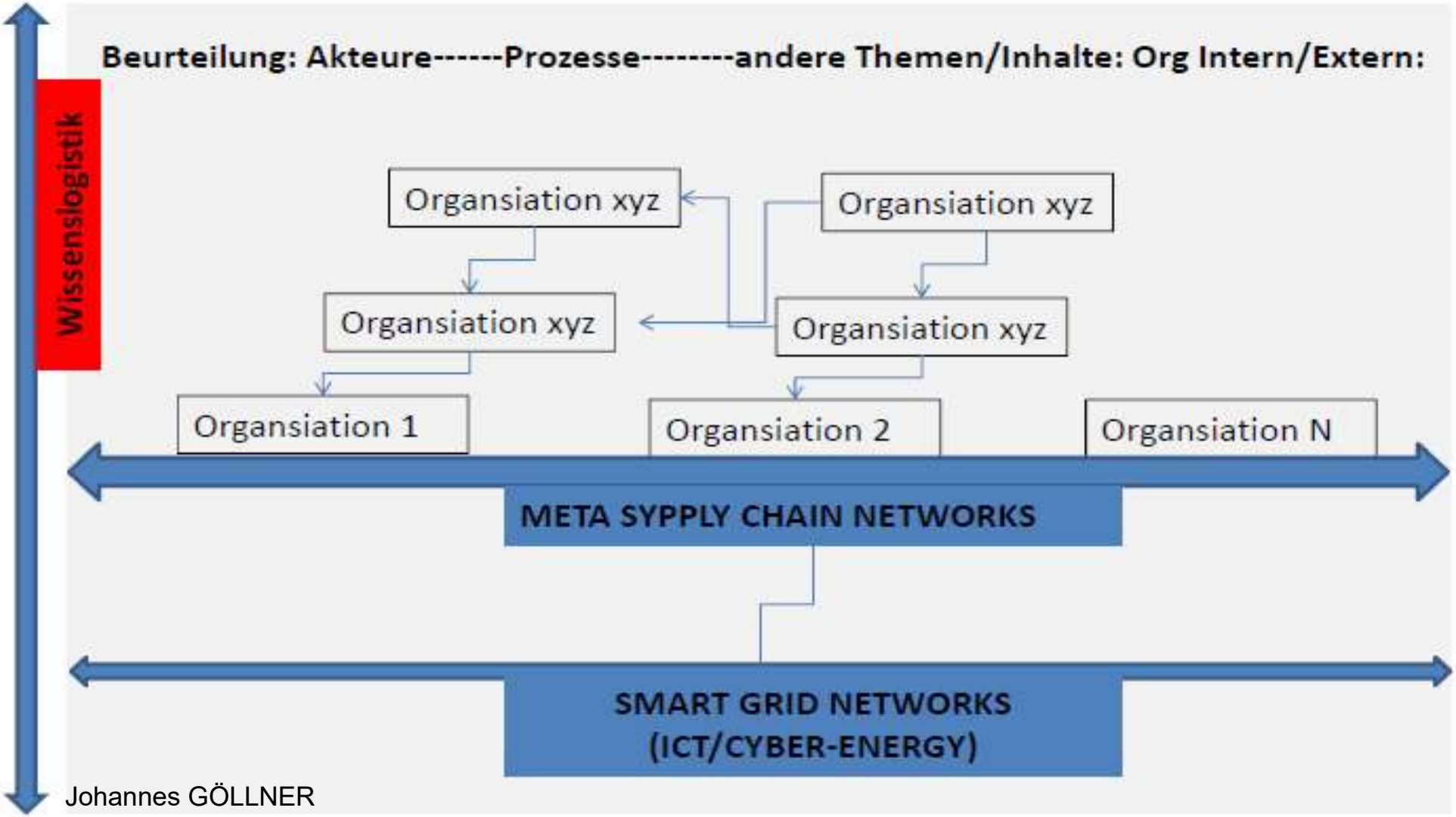
I. Basic Networks

- 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

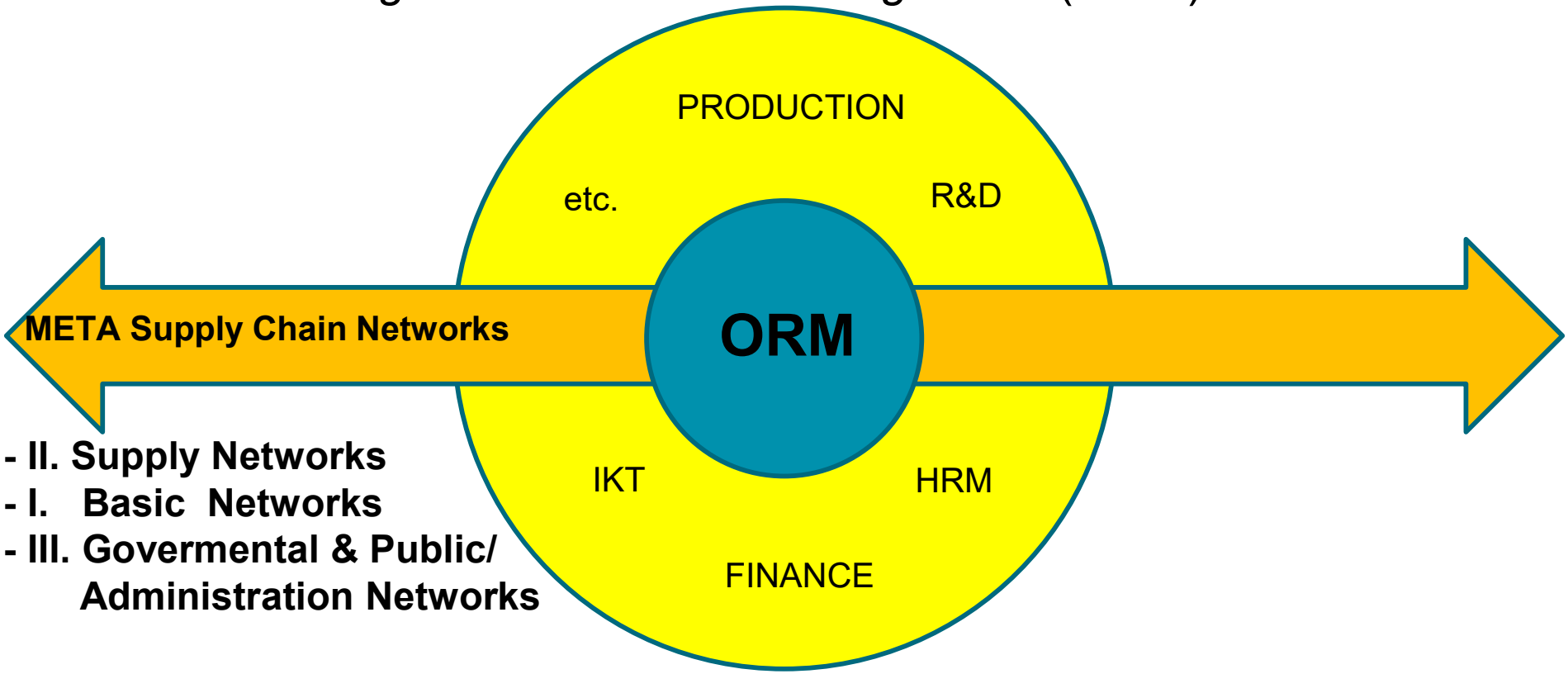


Johannes GÖLLNER

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)

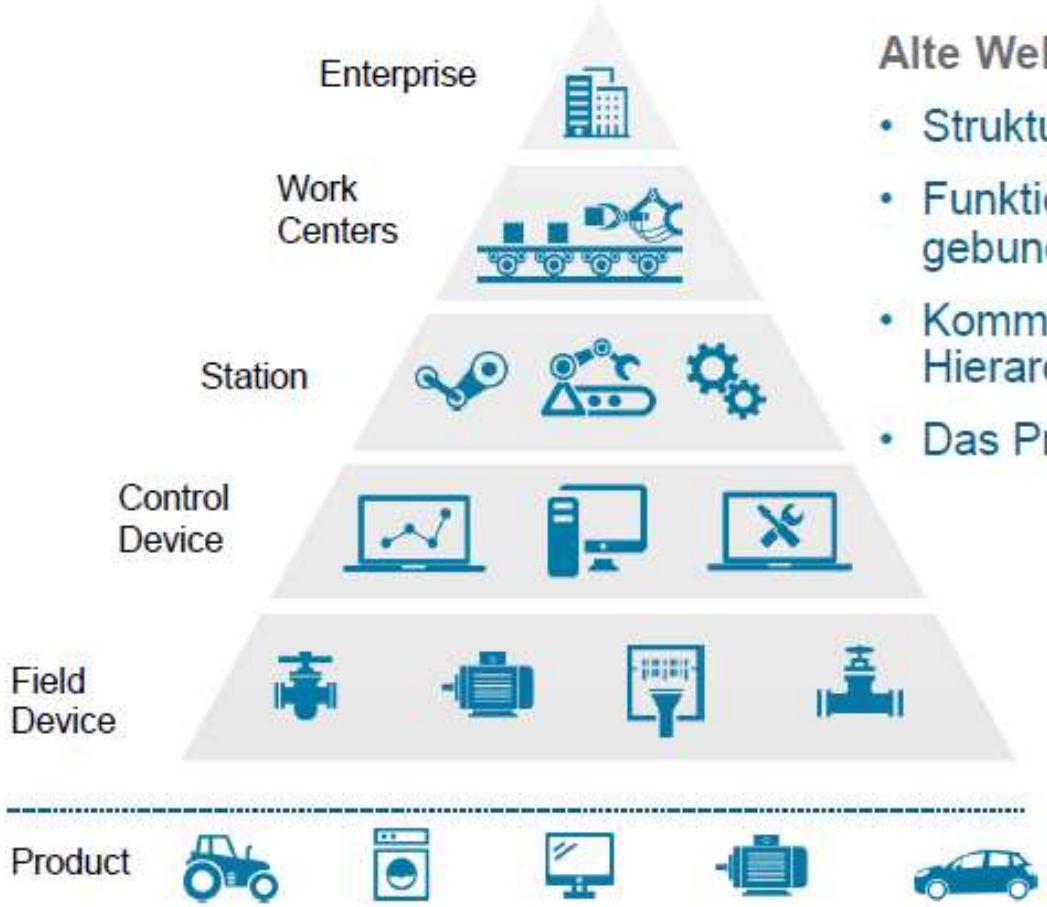


- **II. Supply Networks**
- **I. Basic Networks**
- **III. Govermental & Public/ Administration Networks**

relation: Organisation – Supply Chain Networks – ORM, J.Goellner

PLATTFORM INDUSTRIE 4.0

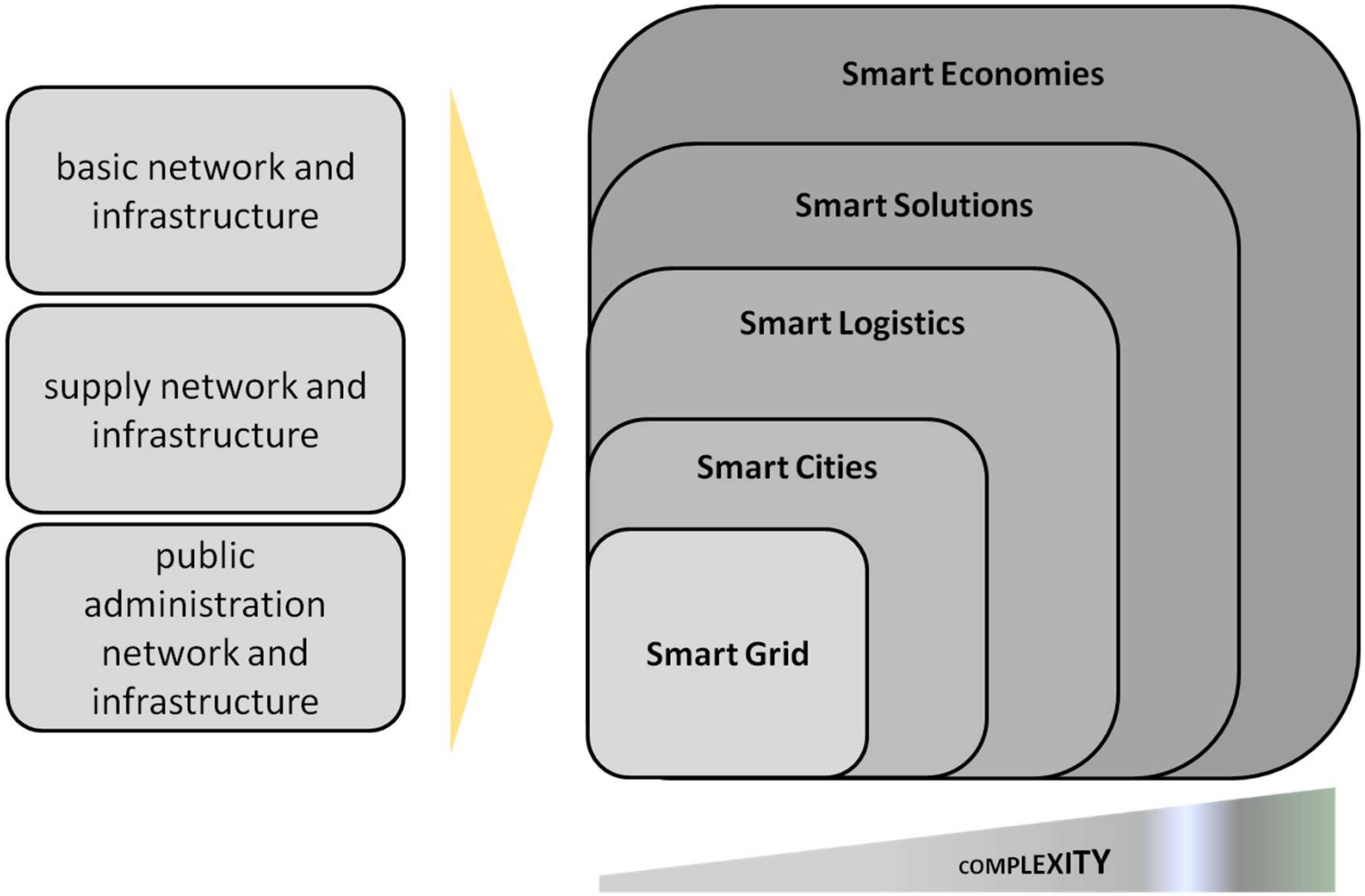
Achse 1 – Hierarchie – Die Fabrik



Alte Welt - Industrie 3.0

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

Global Supply Chain Networks



II. NIS-2 Richtlinie:

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.**

II. NIS-2 Richtlinie:
NIS-2: Wesentliche und Wichtige Einrichtungen

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	

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.

III. Wechselwirkungen zu anderen relevanten EU directives, Gesetzen, Standards, Leitfäden und Publikationen: (*auszugsweise)*

Regelwerke: *auszugsweise:*

1. *Gesetze: z.B.*
2. **Standards: (intern./national), z.B.:**
   - ***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;*
   - **ISO 22361** *(Security and resilience — Crisis management — Guidelines), First edition 2021-11-05; aktueller Stand: ISO 22361:2022;*

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;

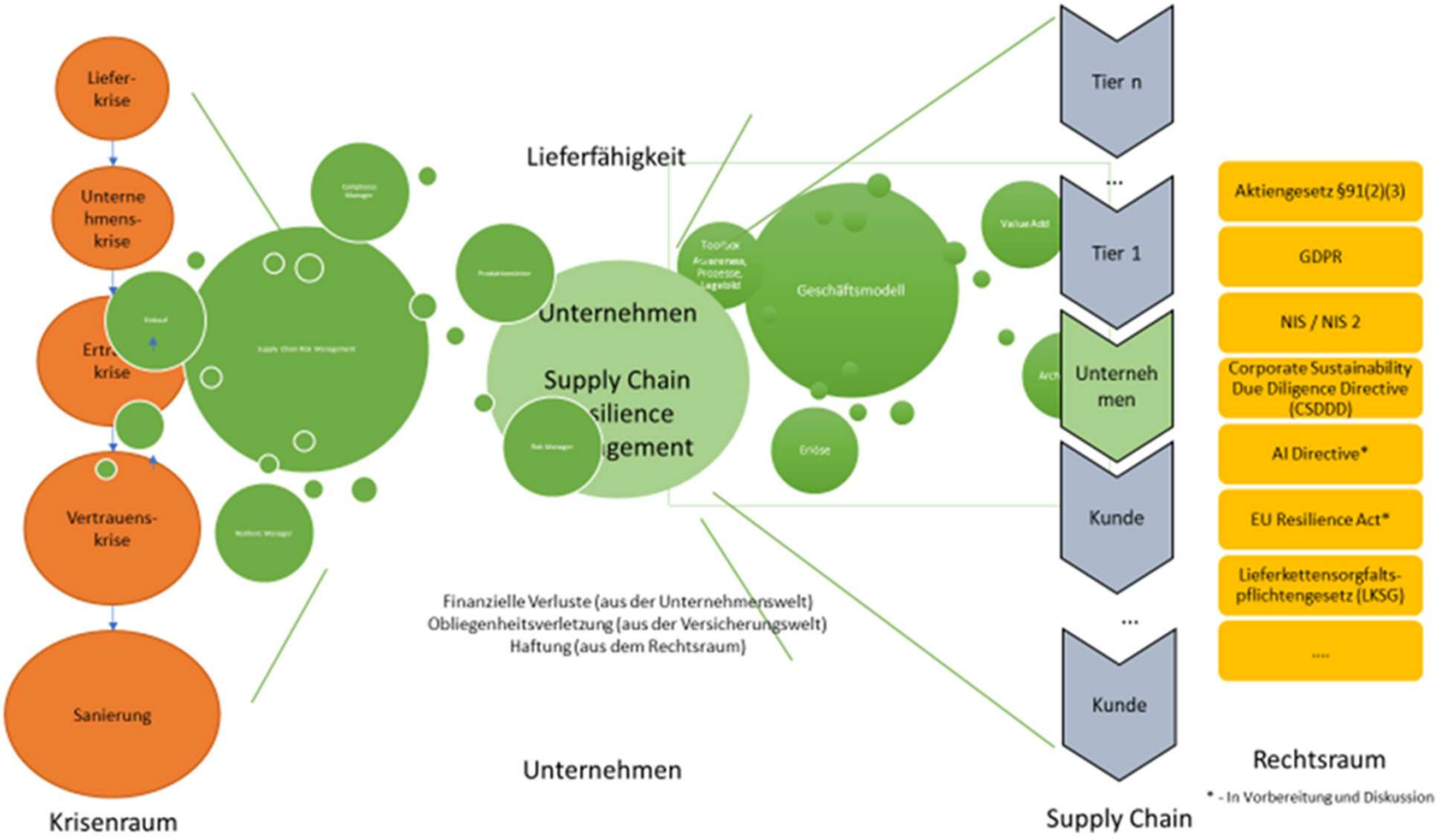
(g) basic cyber hygiene practices and cybersecurity training;

(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.

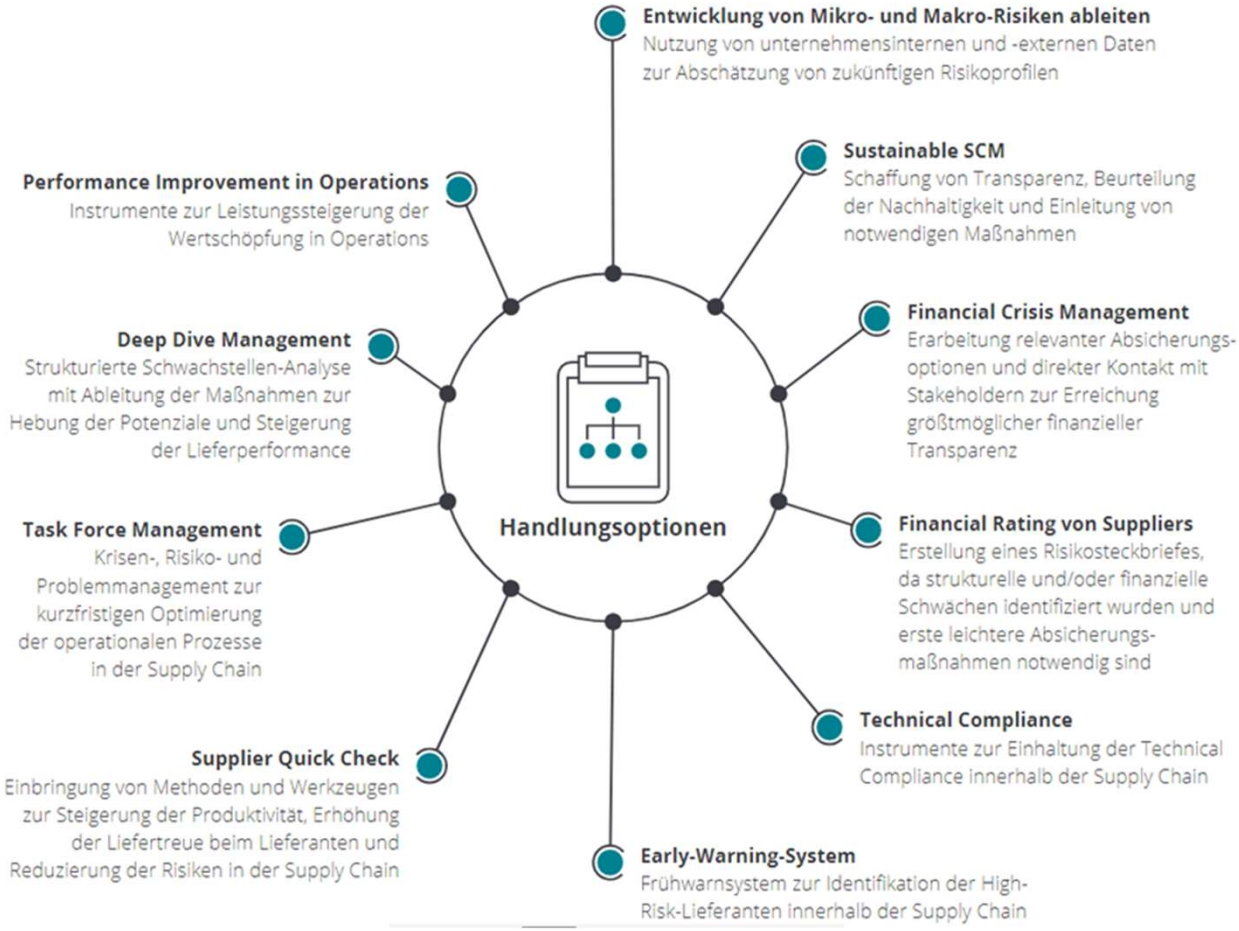
RMA Leitfaden:
SUPPLY CHAIN RESILIENZ MANAGEMENT



RMA Risk Management & Rating Association e.V.

Lösungsansätze: Beitrag RMA e.V., AK SCRM

RMA Leitfaden: Veröffentlichung: 12/2023 (expected)
SUPPLY CHAIN RESILIENZ MANAGEMENT



RMA Risk Management & Rating Association e.V.

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

Regelwerke:

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

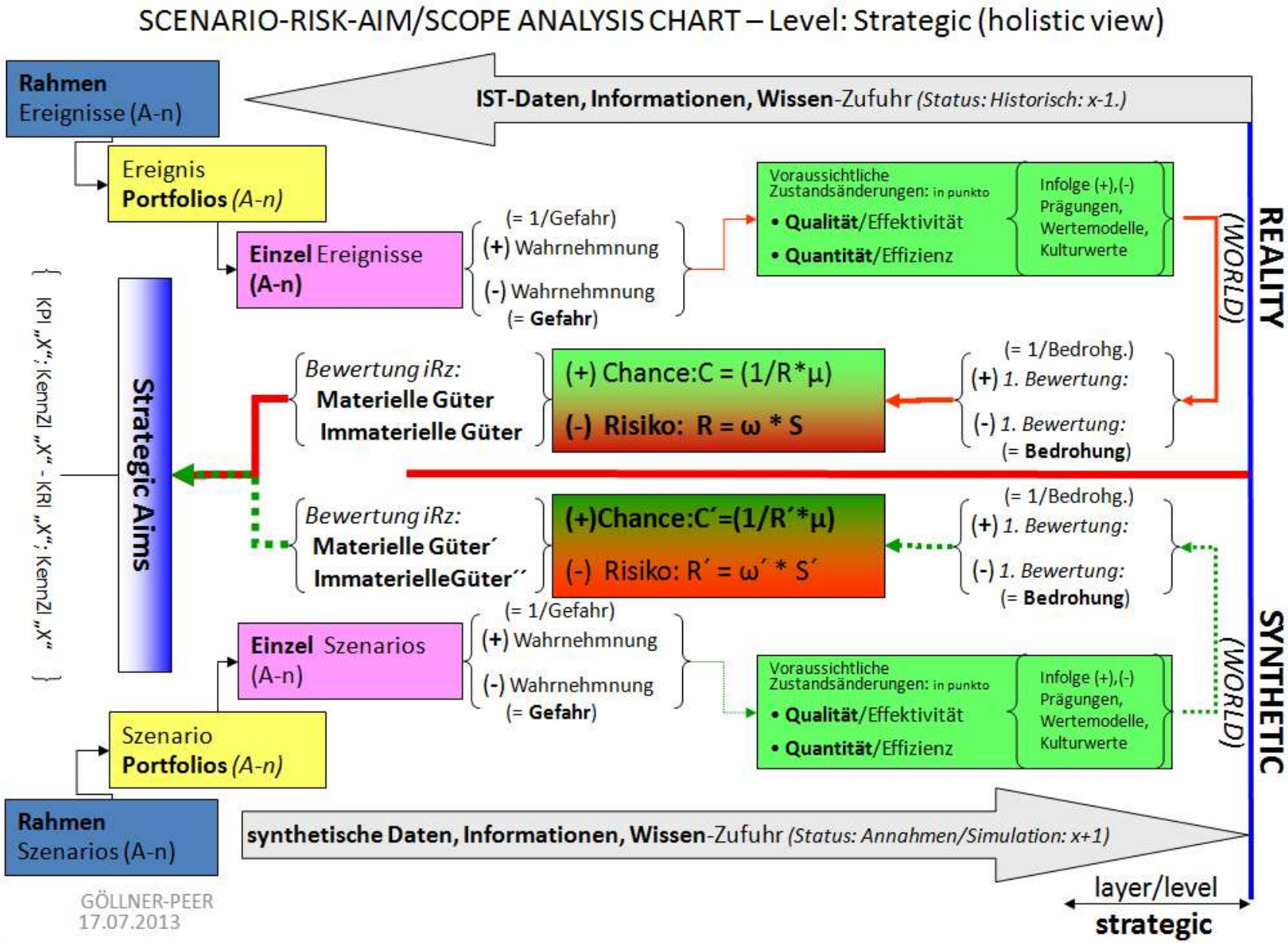
- **Leitfaden für Supply Chain Risk Management (der Risk Management Rating Association-RMA e.V.,**
- **Version 1: Stand 2015)**

Link 1: Supply Chain Risk Management: RMA Risk Management & Rating Association (rma-ev.org)
Link 2: Leitfäden - Zentrum für Risiko- und Krisenmanagement (zfrk.org)

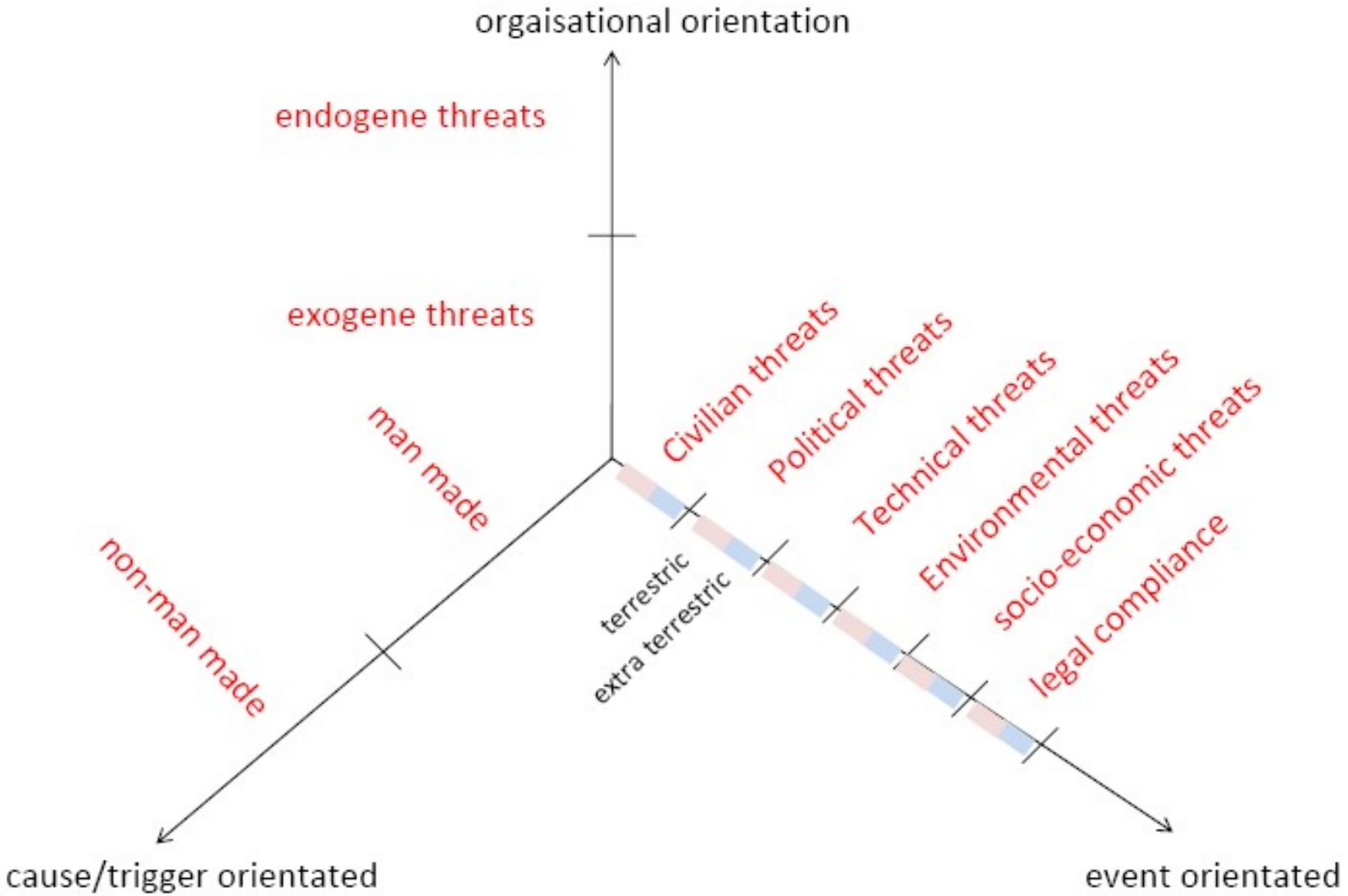
- **Risky Business:What Supply Chain Disruptions Really Cost, Everstream Analytics,** *02.02.2022*

Link 1: Special Reports - Everstream AI

Towards an integrated model: „RPMS CYBER/ICT-SCR“

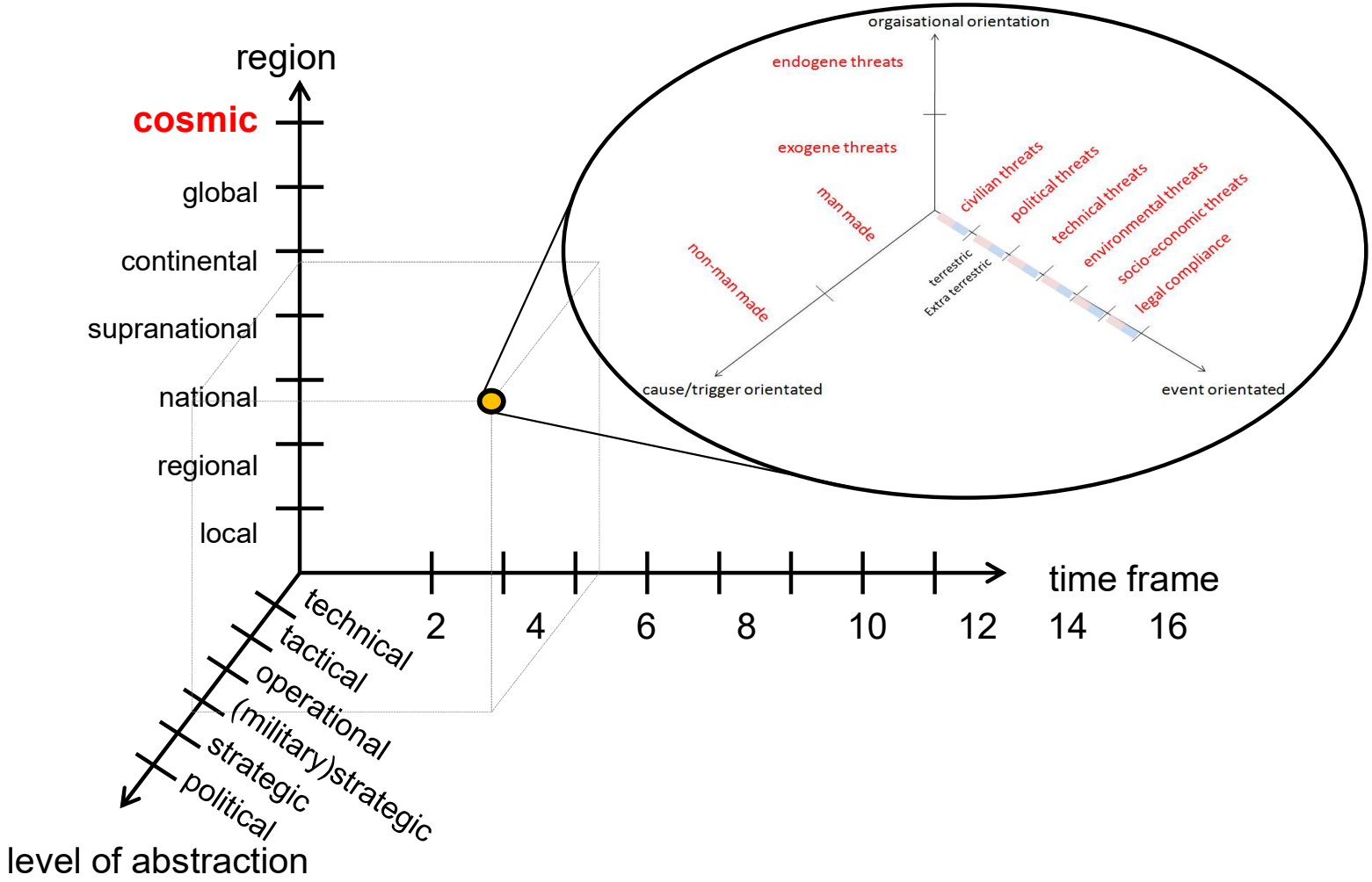


Meta Model of an Organisation



27

Multilayer Vector Model - Basis for Decision Making



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

28

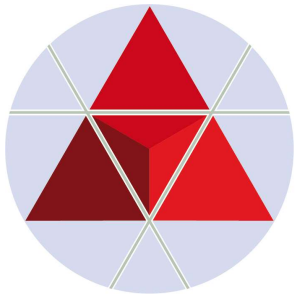
Kontakt:

DI Johannes GOELLNER
Vorstandsvorsitzender &
Ltr RMA-AK-SCRM der RMA e.V., München
Zentrum für Risiko- und Krisen Management (ZRK)
A-1180 Vienna, Reisnerstrasse 5/20a, Austria
M: +[43]-650-2252991
email: johannes.goellner@zfrk.org

Ralf A. HUBER
Mitglied des RMA-AK-SCRM &
Vorstandsmitglied RMAe.V., München
München
email: ralf.huber@rma-ev.org

Zentrum für
Risiko- & Krisenmanagement

RMA
Risk Management & Rating Association e.V.



Zentrum für
Risiko- & Krisenmanagement

Thank you for your attention.

excellent.
connected.
individual.