Expert Talks 2026

EUROPÄISCHE RESILIENZ: HANDLUNGSFÄHIGKEIT UNTER DRUCK SICHERN

Dipl.-Ing. Helmut Leopold, PhD
Chair Gaia-X Hub Austria
Head of Center Digital Safety & Security
AIT Austrian Institute of Technology

Wien, 8. Oktober 2026
(v1.0)

DIGITALE SOUVERÄNITÄT

Definition

- Unabhängiges und selbstbestimmtes Handeln im digitalen Raum
- Wahlfreiheit statt Abhängigkeit
- Kontrollmöglichkeit über Daten und Cloud-Services (KI Agenten)

Warum entscheidend?

Demokratie & Sicherheit
Schutz vor externem Zugriff & Einfluss

Wettbewerbsfähigkeit
Daten und Cloud Services als Grundlage für Innovation

Technologische Unabhängigkeit
Reduktion globaler Abhängigkeiten

Europäische Werte
Technologien nach eigenen Prinzipien

KI & Innovation
Grundlage für effektive KI-Anwendungen und Innovationen

Digitale Souveränität = Voraussetzung für Sicherheit und Innovation in Europa und damit für Demokratie und für eine wettbewerbsfähige Wirtschaft.

RESILIENZ ALS NEUE SOUVERÄNITÄT

- Resilienz ist kein rein defensives Konzept - Schutz vor Angriffen, sondern verlangt umfassende Mechanismen zur nachhaltigen Sicherstellung einer strategischen Handlungsfreiheit.
- Wer erpressbar, manipulierbar oder alternativlos ist, hat keine souveräne Handlungsfreiheit!

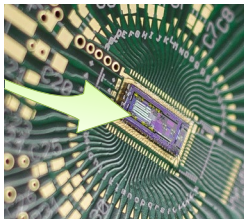
Cybersecurity

Resiliente kritische Infrastrukturen



Technologische Unabhängigkeit

Reduzierung von Risiken bei Halbleitern, kritischen Rohstoffen und IT Lösungen.



Next Gen Internet – Souveräne Datenräume

Governance & compliance – Daten. Cloud-Services, KI Agenten (Qualität, Trust, ethische Werte)



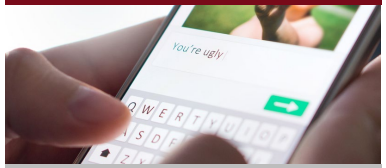
Mitgestaltung von Markttreiber

Standards, Governance, Compliance & **effektive Umsetzung**



CYBERSECURITY - THREAT LANDSCAPE

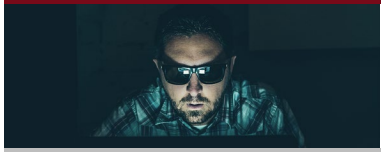
Cyber Bullying



Fake News

Bullying, Staking, rumors, hate speech, Slander

Cyber Crime



Ransomware

CEO Fraud, extortion, fake shops, fake trading

Cyber Terrorism



Critical infrastructure attacks, sabotage

Disruption of essential national services

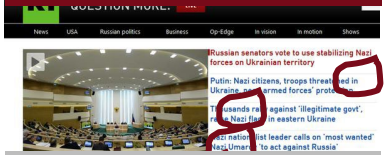
Cyber Espionage



Industrial espionage

Economic espionage – state sponsered

Disinformation



Narratives for public opinion, de-stabilization

influence of elections – state sponsered

Hybrid operations



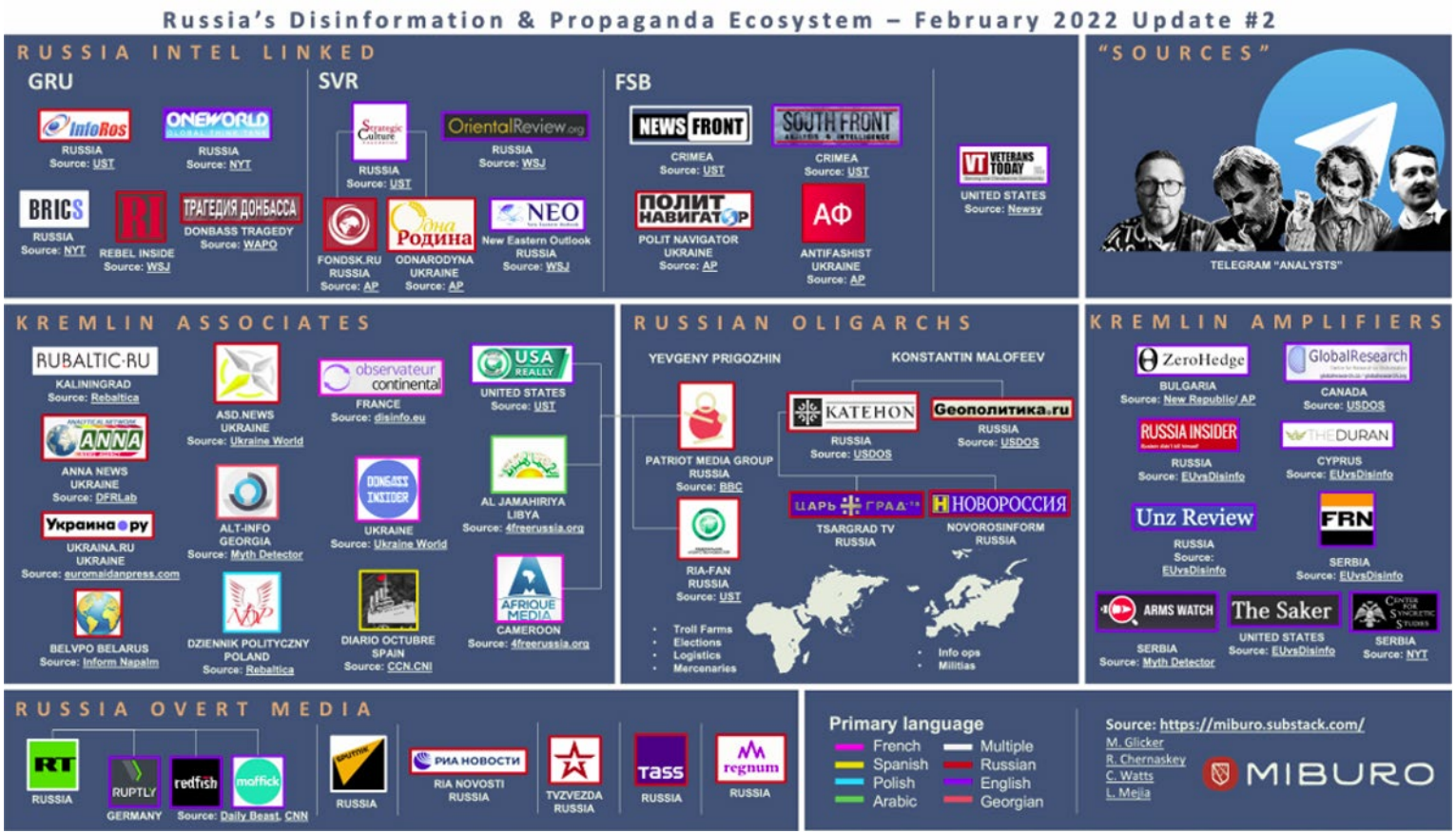
Cyberattacks combined with, sabotage and disinformation (influence)

THREAT ACTORS – 140 ACTIVE APT GROUPS WORLDWIDE

	APT1 / Comment Crew, APT10 / MenuPass, APT27 / Emissary Panda, APT40, APT41, Volt Typhoon, Salt Typhoon	Strategic espionage, government, defense, technology, telecommunications and critical infrastructure
	APT28 / Fancy Bear, APT29 / Cozy Bear, Sandworm / APT44, Turla, Gamaredon	Government and military intelligence, diplomatic organizations, defense, critical infrastructure, Ukraine-related targets
	Lazarus, Kimsuky, Andariel, BlueNoroff	Intelligence collection, defense/technology, cryptocurrency and financial theft
	APT33 / Elfin, APT34 / OilRig, APT35 / Charming Kitten, MuddyWater, Agrius	Government, defense, energy, telecommunications, regional adversaries and intelligence collection
	APT32 / OceanLotus	Espionage involving governments, corporations and organizations of strategic interest
	APT36 / Transparent Tribe	Government, defense, diplomatic and regional intelligence targets
	Multiple India-linked groups, including Patchwork and SideWinder	Regional government, diplomatic and strategic intelligence targets
	Sea Turtle, StrongPity	Telecommunications, government and regional targets

AIT research: BSI, Microsoft, MITRE, Mandiant publications

DAS DESINFO TROLL ECO-SYSTEM



CYBERSECURITY IS A YOUNG COMPUTER SCIENCE DISCIPLINE – MALWARE SIGNATURES

- **400 k Vulnerabilities –**
  200 new per day



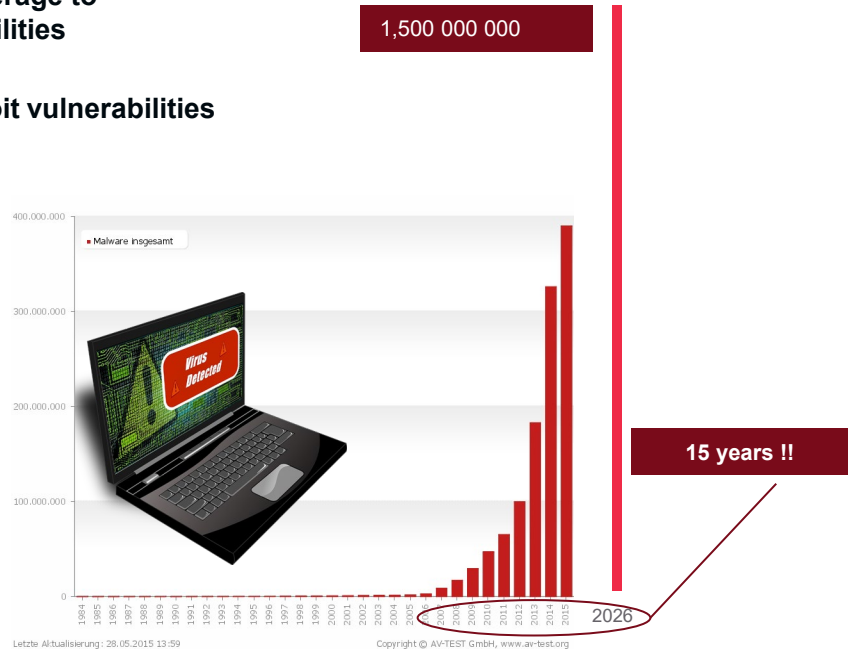
176 days in average to close vulnerabilities



7 days to exploit vulnerabilities → 0 days → AI!

- **200 k new malware variants per day** (Viruses, Worms, Trojaner)
- **Daily 10 k** new websites with malware for download
- **Malware is already adpting** to „Antivirus-SW“ („change of signatur“)

- **Spam** – **75-90%** of the global e-mail traffic



Source: AIT research, BSI/2026

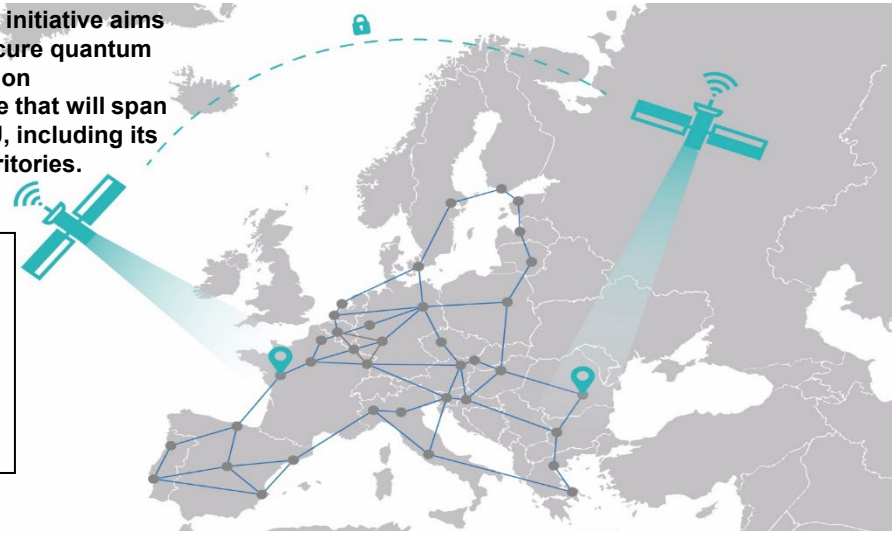
TECHNOLOGISCHE UNABHÄNGIGKEIT

EU DATA SOVEREIGNTY THROUGH QUANTUM KEY DISTRIBUTION (QKD)

AUSTRIAN INSTITUTE OF TECHNOLOGY

EuroQCI

The EuroQCI initiative aims to build a secure quantum communication infrastructure that will span the whole EU, including its overseas territories.



- EU Scientific & Industrie Leadership in Quantum Technology
- EU Security Strategy
- EU Infrastructure Strategy
- EU Industry Strategy

IRIS², Europe's new Infrastructure for Resilience, Interconnection & Security by Satellites



Press Releases:

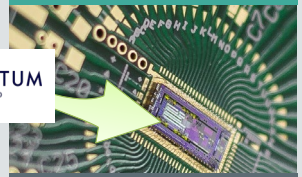
EuroQCI:
- https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

IRIS²:
- https://www.consilium.europa.eu/de/press/press-releases/2022/11/17/council-and-european-parliament-agree-on-boosting-secure-communications-with-a-new-satellite-system/
- https://www.nzz.ch/technologie/iris2-die-eu-baut-ein-eigenes-satellitensystem-fuer-sicheres-internet-ld.1712855
- https://orf.at/stories/3305570/
- https://defence-industry-space.ec.europa.eu/system/files/2023-02/IRIS%C2%B2_Factsheet%20%28DE%29.pdf

EuroQCI – Quantum Communication Infrastructure Europe, **2019-2029**

AIT AS A KEY DRIVER FOR THE EU QKD/PQC QUANTUM ECO-SYSTEM

QUANTUM FLAGSHIP

R&D - HW & SW	Consulting	Standardization	Space	EU 27 SMEs & Industry
		CEN CENELEC, ITU, ETSI		https://quantum.ait.ac.at/ fragmentiX, DEP eCAUSIS, DEP Quarter
QKD Miniaturization on the Chip	Extensive Know-How for EU QKD Eco-System	Key advisor for the EU Commission in industry standardisation strategy	Technology supplier for the EU Industry	EU Industry & Market Support

- R&D
- Technology supply within EU
- Infrastructure services
- EU Eco-System development

EU Satellite launch:
2027 Eagle in Orbit
2028 SAGA in Orbit

AUSTRIAN INSTITUTE OF TECHNOLOGY

Test & validation of technology (Nostradamus)

THALES

EU Industry & Agency Support

Enablement of the Austrian & EU Eco-System

QKD4Gov	QCI-CAT	DEP Petrus	Connecting European Facilities (CEF)

- Federal Ministry Innovation, Mobility and Infrastructure Republic of Austria
- Bundesministerium Bildung, Wissenschaft und Forschung
- Bundesministerium Arbeit und Wirtschaft
- Federal Chancellery Republic of Austria
- Federal Ministry Republic of Austria Interior
- Federal Ministry Republic of Austria European and International Affairs
- Federal Ministry Republic of Austria Defence

HarmoniQCI is a coordination and support action on the standardisation efforts for EuroQCI.



36 months	06/2026–05/2029	95%	€2.991m
Project duration	Project period	Funding rate	Max EU grant

Main Goal

Facilitate and intensify the standardisation activities at **all levels** for an operational EuroQCI

Project Mission

The project aims to ensure the **integration** of quantum communication technologies into telecommunication networks (including the space segment), with a focus on interoperability, security protocols, and QKD components and systems

Partners

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

DEUTSCHE TELEKOM

Telefónica

ses

POLITÉCNICA

TNO

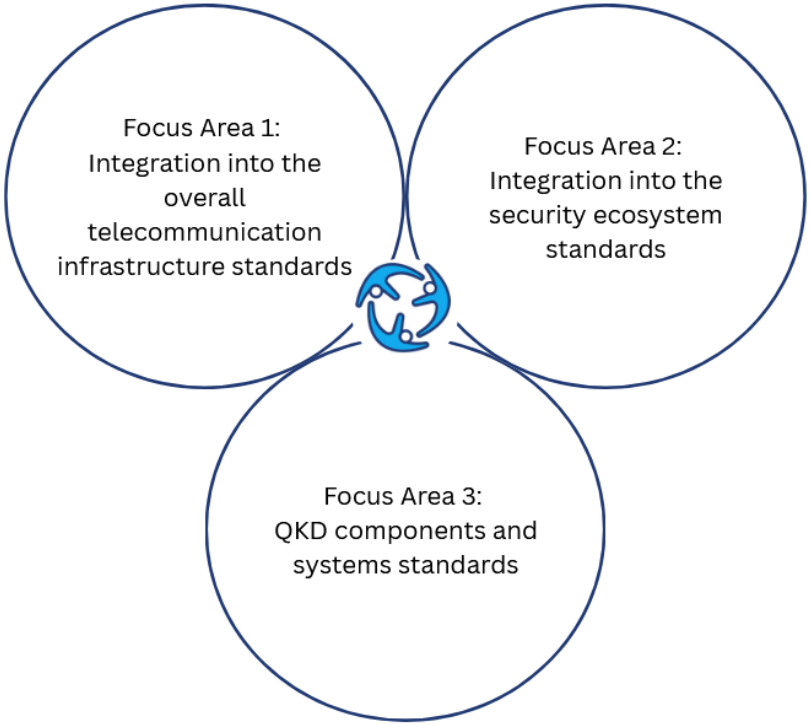
SYNDESIS

ETSI

UIC

UNE Normalización Española

HarmoniQCI - Standardization Focus Areas

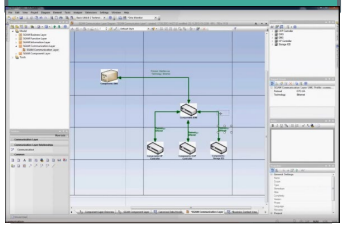


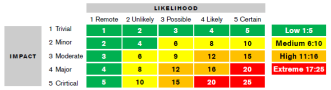
NETX GENERATION CYBERSECURITY SOLUTION PORTFOLIO MADE IN AUSTRIA

AUSTRIAN INSTITUTE OF TECHNOLOGY

Protecting critical infrastructures, fighting Cyber Crime & Terrorism

Safety & Security by Design





INDUSTRIE 4.0 ÖSTERREICH

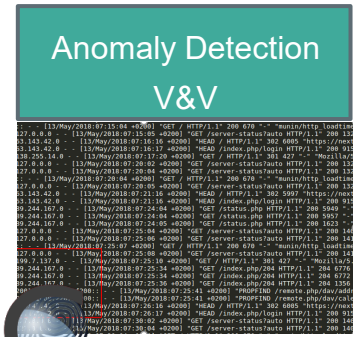
AVL

LieberLieber

THREATGET

www.threatget.com

Anomaly Detection V&V





- AI based penetration tests
- Logfile analyses
- OT system analysis
- Run-time verification
- Post Quantum Encryption

ÆCID

www.aecid.ait.ac.at

Security Operation Center (SOC)

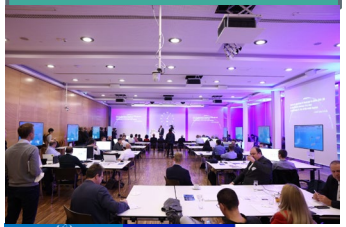




TARANIS_AI

https://taranis.ai/

Cyber Security Capacity Building





KSÖ Kompetenzzentrum Sicheres Österreich

EDIC-CSC

NCA

CYBER RANGE

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

www.cyberrange.at

Countering Desinformation



Fighting Online Crime

Fake-Shop Detector

https://www.fakeshop.at/

INTERNATIONAL LEADING TECHNOLOGY FROM AIT

DIGITAL IDENTITY – CONTACTLESS BIOMETRICS

Federal Ministry Interior

March 2026

UNITED NATIONS OFFICE OF COUNTER-TERRORISM

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

Responsible Biometrics for Digital Based Border Management

https://responsible-biometrics.org/

World Border Security Congress

April 2026

UNOCT

New York

July 2026

A new platform to share recent developments and innovative, science-based solutions for secure border management, in compliance with Human Rights and technical standards applicable to new technologies. The contents of this platform are the result of the cooperation between the AIT Austrian Institute of Technology and the Counter-Terrorism Centre of the United Nations Office of Counter-Terrorism.

KIRAS Sicherheitsforschung

Bundesamt für Sicherheit in der Informationstechnik



BMI+AIT - UN best practice example for responsible digital technology development

gaia-x
Hub Austria

Accelerating European Data Ecosystems for economic, ecological and societal value creation.

Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria

Federal Chancellery
Republic of Austria

State Secretariat for
Digitalisation

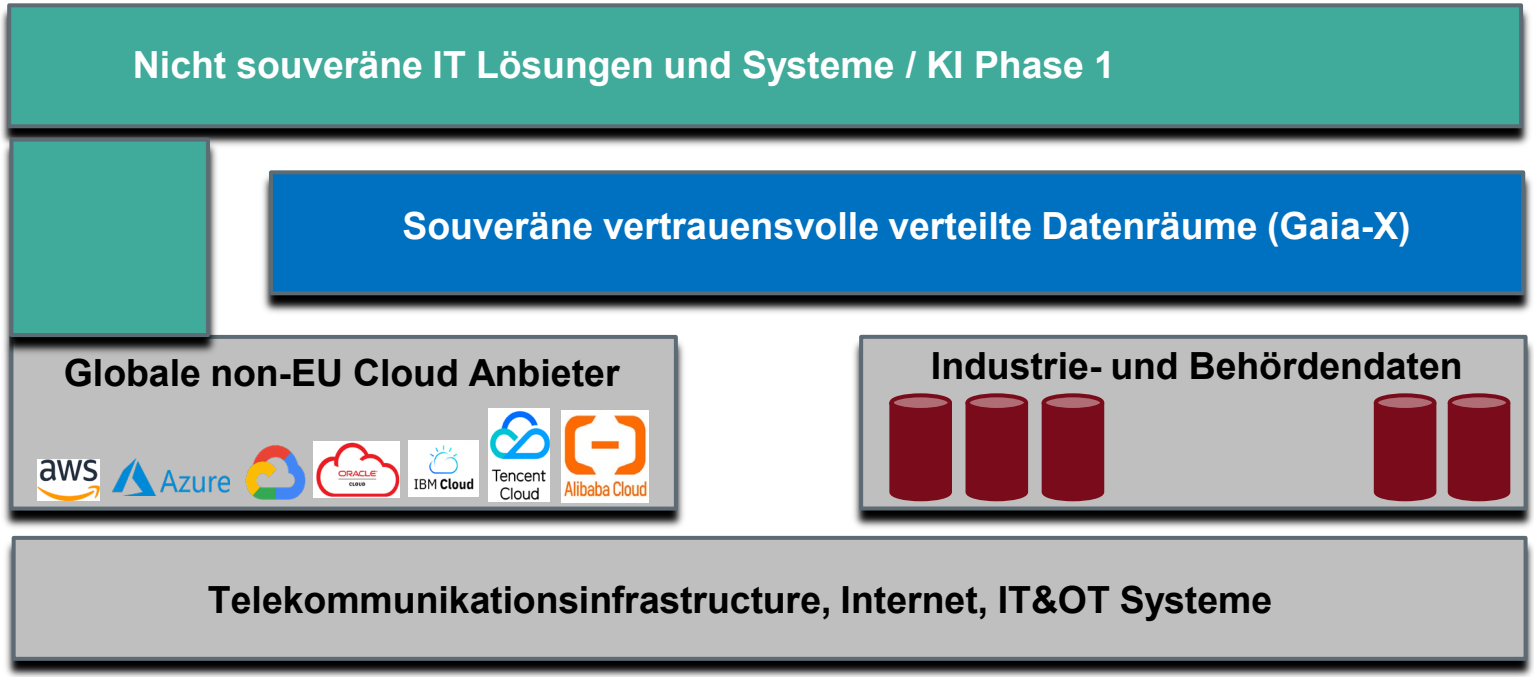
UNTERSCHÄTZER WETTBEWERBSFAKTOR – COMPLIANCE, QUALITÄT UND TRANSPARENZ

- NIS-2
- DORA
- EU Directive 2022/2557 on the Resilience of Critical Entities
- Cyber Resilience Act (CRA)
- Data Act
- Data Governance Act
- AI-Act
- Digitaler Produktpass
- Öko-Design Verordnung
- Supply Chain Sicherheit
- Domänenspezifische Regeln
- …



- Transparenz und Nachvollziehbarkeit – Daten, Cloud Services, Open Source, KI Agenten, …
- Effektive Zertifizierungsprozesse
- Automatisierte Überprüfbarkeit

VOM INTERNET ZUM SOUVERÄNEN DATENGESCHÄFT UND AUTOMATISIERTE COMPLIANCE

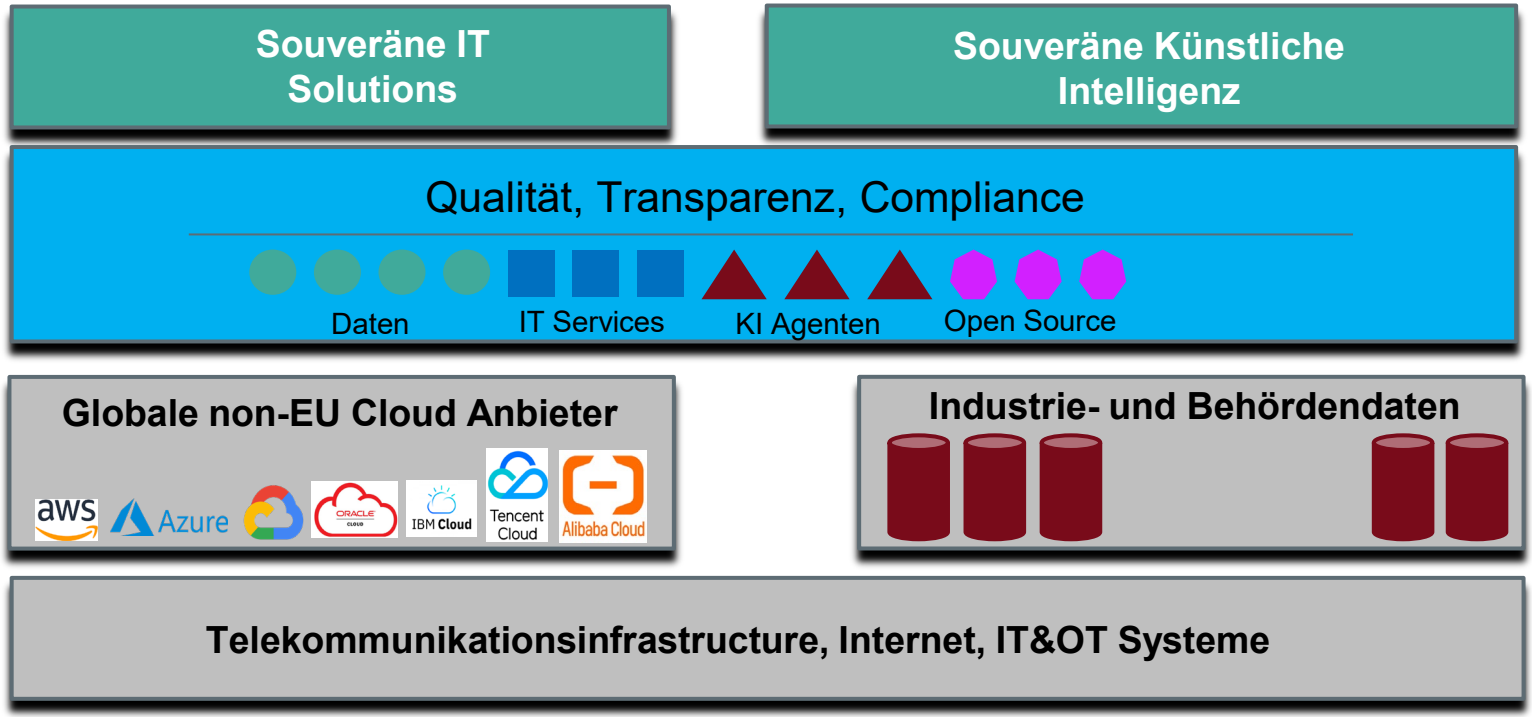


Daten-speicherung

Economy of scale

Breitband Infrastruktur

VOM INTERNET ZUM SOUVERÄNEN DATENGESCHÄFT UND SOUVERÄNEN IT SERVICES



Gaia-X Summit, 19.11. – 20.11.26, Vienna

Demonstration of Austria as an essential shaping MS in the EU on the topic of data sovereignty

- ✓ **Motto**: Season 2.0 of Sovereign, Trusted AI & Data Ecosystems
- ✓ Gaia-X Hub Austria as host
- ✓ **Europe's Central Conference on Data Spaces, Digital Sovereignty and Trusted Cloud & Data Infrastructures**.
- ✓ **Gaia-X flagship event** for industry, research and politics with best practices, tech sessions and networking on the topic of data sovereignty, data spaces and Gaia-X.
- ✓ **Presentation of Austrian. Innovation & Data Industry**
- ✓ **Programm**: https://gaia-x.eu/event/gaia-x-summit-2026/



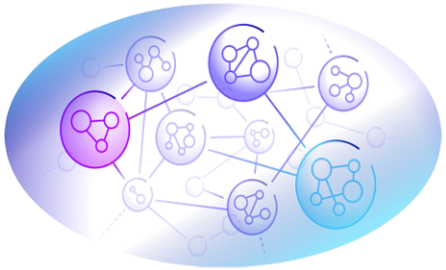


DIGITALE SOUVERÄNITÄT - HANDLUNGSFELDER

Resilienz kostet Geld und erfordert Investitionen. Diese Kosten sind eine Versicherungsprämie für unsere Demokratie und Freiheit

- **Hohe Cybersicherheit** → hohe Resilienz der digitalen Infrastrukturen
- Kompetenzen und Werkzeuge für den Kampf gegen **Desinformation** und Fake-News
- **Umsetzbare Governance** → ethische Werte, freie Märkte
- **Automatisierte Compliance und souveräne EU Datenräume** (Gaia-X)
- Offene **Standards** → globale Standardisierung
- Verstärkter Einsatz von **Open Source**
- **Berufliche Weiterentwicklung** („upskilling) → EU Cyber Skill Academy

Neue Ökosysteme



Kooperation aller Stakeholder





Industrie, kritische Infrastrukturen



Behörden



KMUs

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

DANKE!

The Center for Digital Safety & Security Team for global leading applied research @ AIT



