
BWI
IT für Deutschland

23. August 2021

BWI
IT für Deutschland

BWI INDUSTRY DAYS

Gemeinsam für die digitale Zukunft der Bundeswehr

23./24. August 2021, Bonn

23. August 2021

Quantum Computing & Kubernetes Bare Metal im Kontext private Cloud Bundeswehr

Markus Hauff
CDO DP Strategic Technology Advisor, BWI

BWI
IT für Deutschland

© C Dustin / Unsplash.com

Themen

Einsatzspektrum & Aufbau der pCloudBw

Herausforderung durch Quantencomputing

Entropy* as a Service

Kubernetes@Bare Metal

*Entropie ist in der Informationstheorie ein Maß für den mittleren Informationsgehalt einer Nachricht.

Themen

Einsatzspektrum & Aufbau der pCloudBw

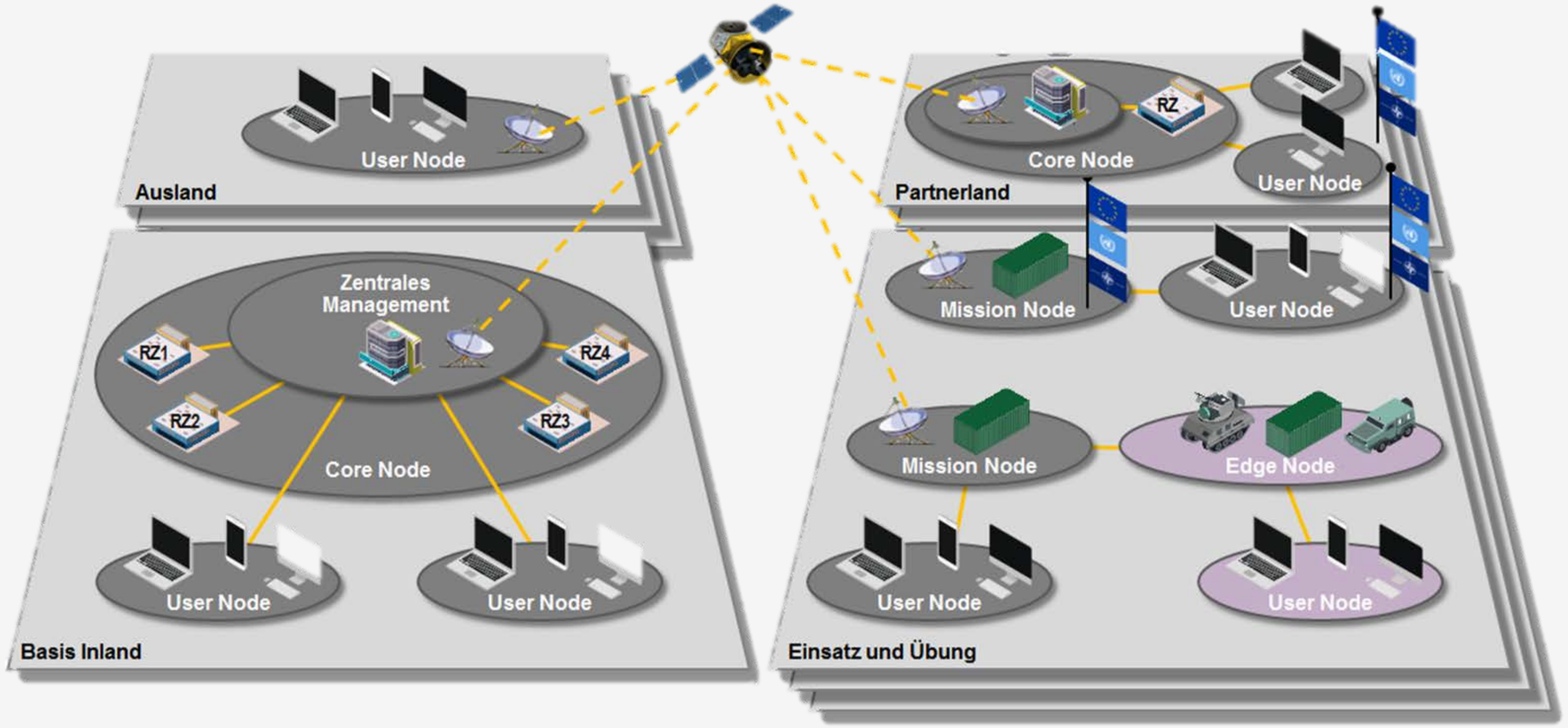
Herausforderung durch Quantencomputing

Entropy* as a Service

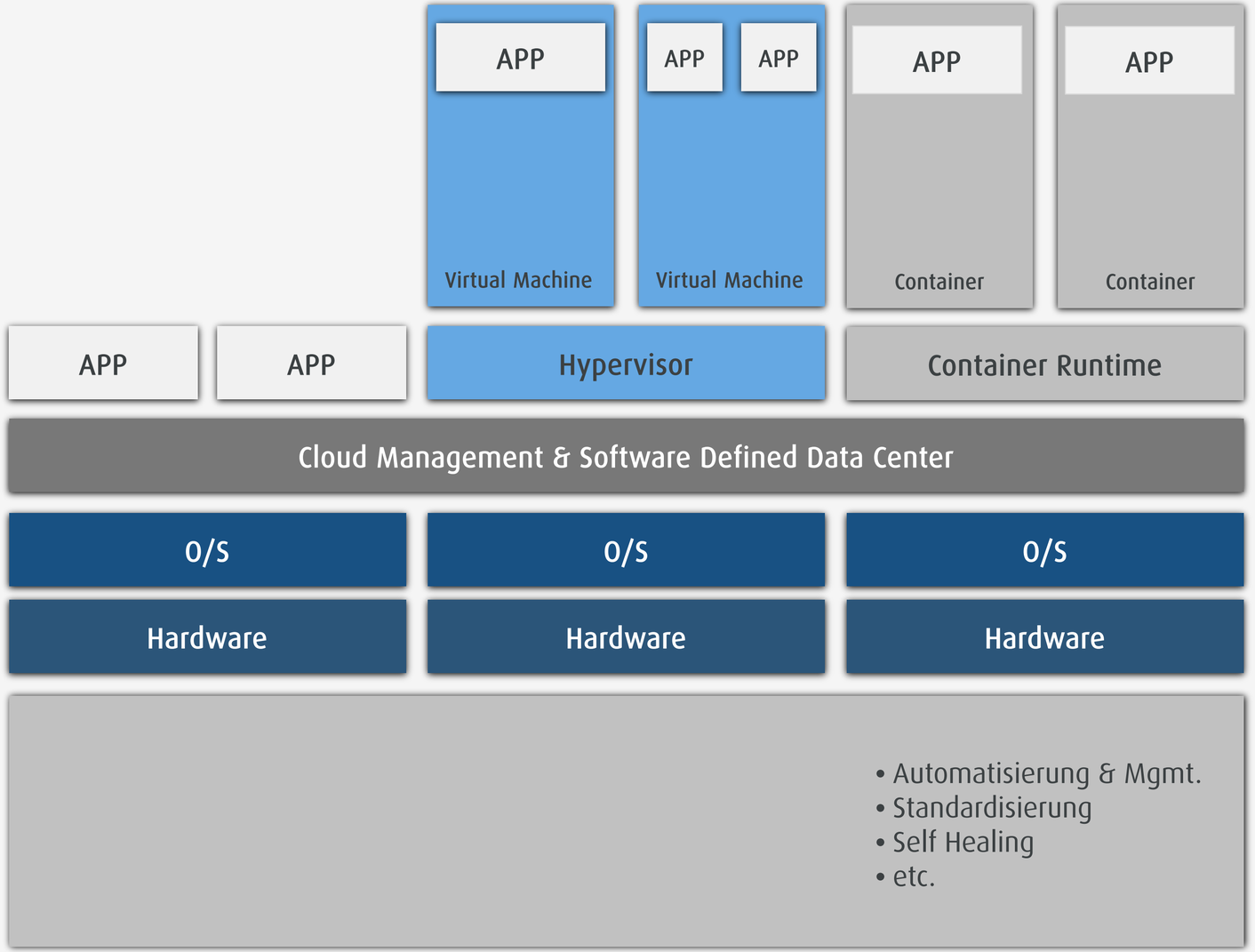
Kubernetes@Bare Metal

*Entropie ist in der Informationstheorie ein Maß für den mittleren Informationsgehalt einer Nachricht.

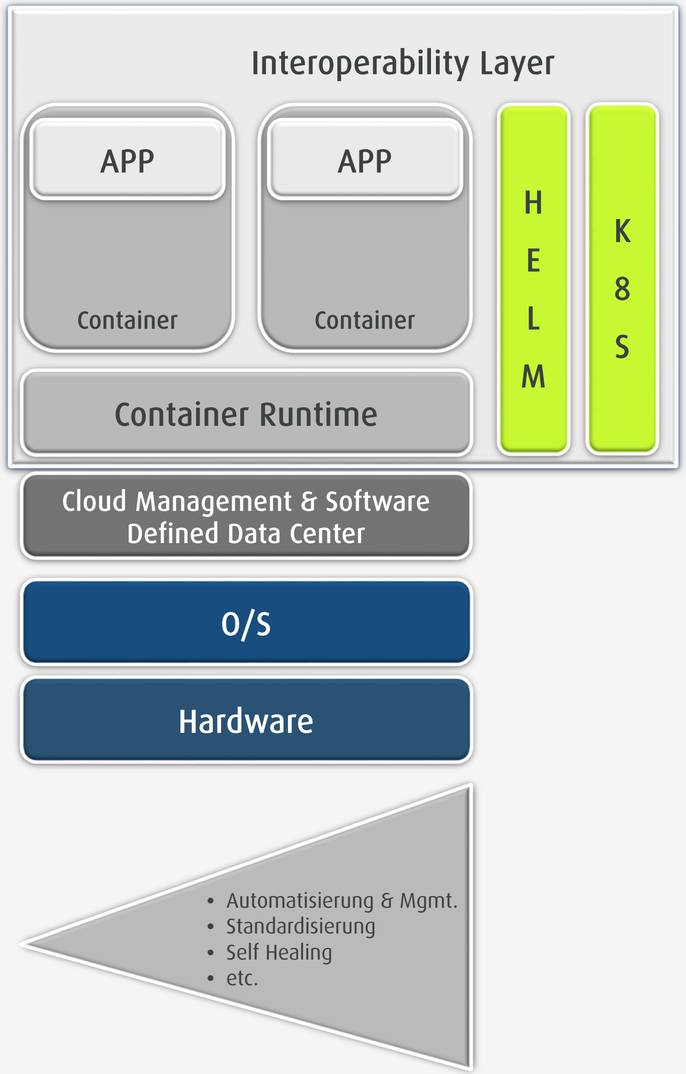
pCloudBw:
Tauglich für alle Einsatzszenarien



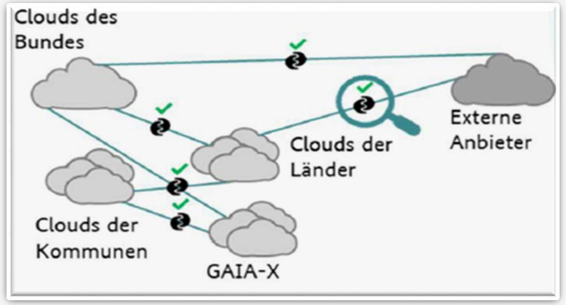
pCloudBw: alles auf einer Plattform



Weiterentwicklung der pCloudBw: **Interoperabilität**



Deutsche Verwaltung Cloud Strategie



NATO Cloud

EDF Multi-Domain Operations Cloud

Combat Cloud

etc.

Themen

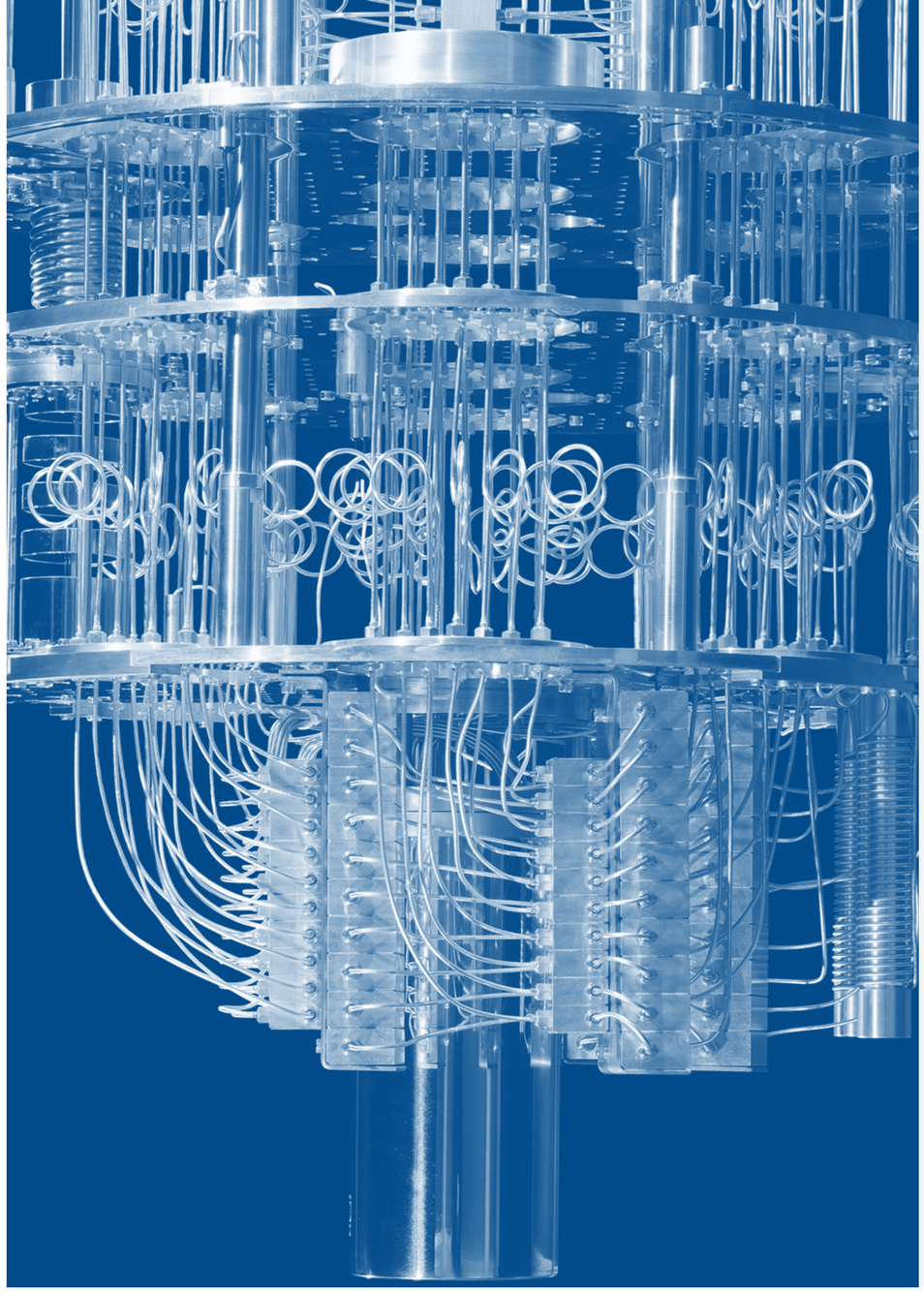
Einsatzspektrum &
Aufbau der pCloudBw

Herausforderung durch Quantencomputing

Entropy* as a Service

Kubernetes@Bare Metal

*Entropie ist in der Informationstheorie ein Maß für den mittleren Informationsgehalt einer Nachricht.

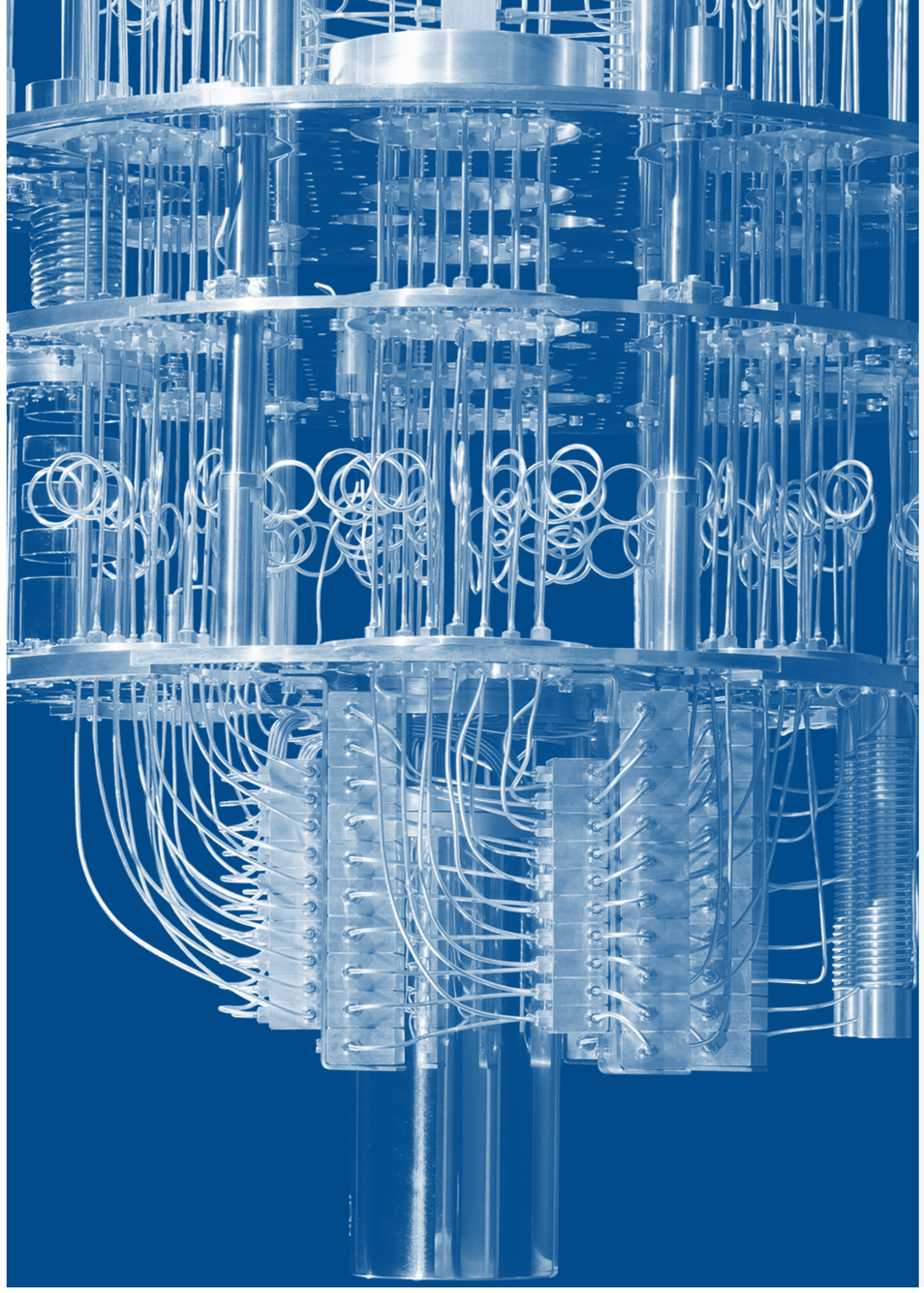


Quantencomputing-Herausforderung für heutige Verschlüsselungssysteme

"In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. **If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use.** This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere."

NISTIR 8105 vom 16. April **2016**
Report on Post-Quantum Cryptography

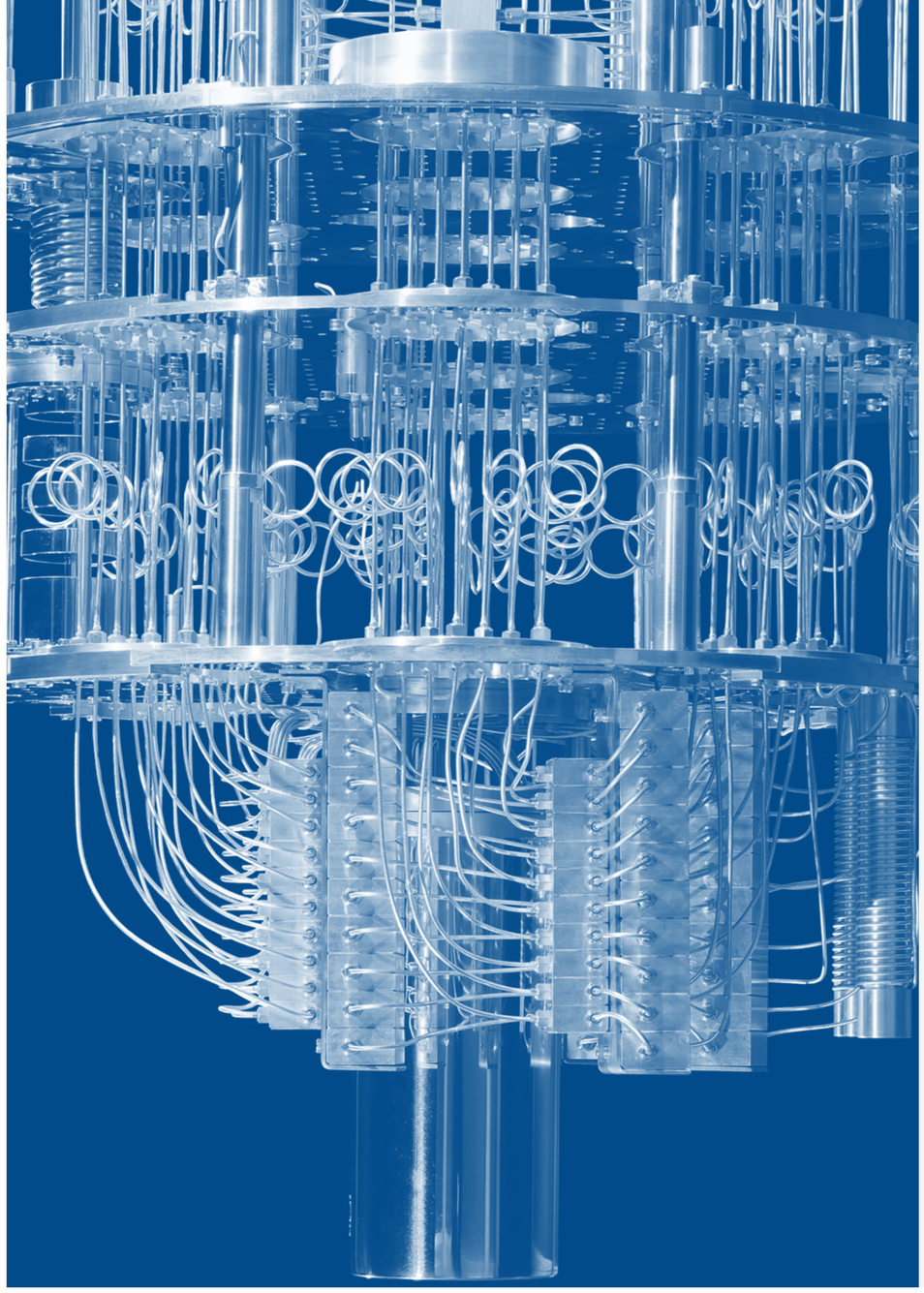
Bild Internet - IBM



Verschlüsselungsalgorithmen werden angreifbar

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Bild Internet - IBM



Industrielle Nutzung Quantencomputer wird Realität

“... If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. ...“

NISTIR 8105 vom 16. April 2016
Report on Post-Quantum Cryptography

September 2020 D-Wave – “Advantage contains at least 5,000 qubits, about 2.5 times more than found in a DWave 2000. The number of couplers per qubit has increased from 6 to 15, for a total of at least 35,000 couplers, representing about a six-fold increase over the earlier system.”

Bild Internet – IBM & D Wave

Themen:

Einsatzspektrum &
Aufbau der pCloudBw

Herausforderung durch
Quantencomputing

Entropy as a Service

Kubernetes@Bare Metal

Bild Internet - mekongnet

Themen

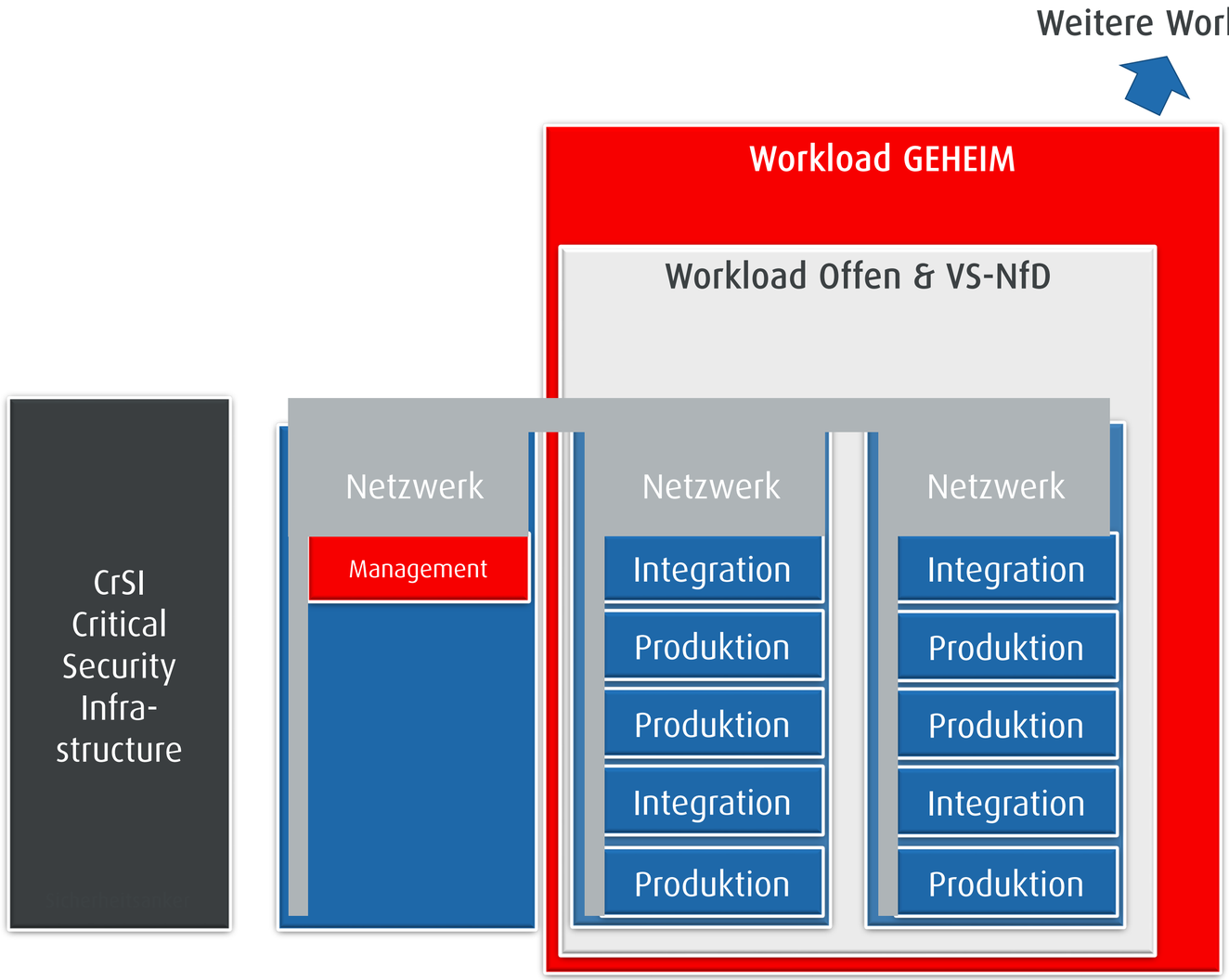
Einsatzspektrum &
Aufbau der pCloudBw

Herausforderung durch
Quantencomputing

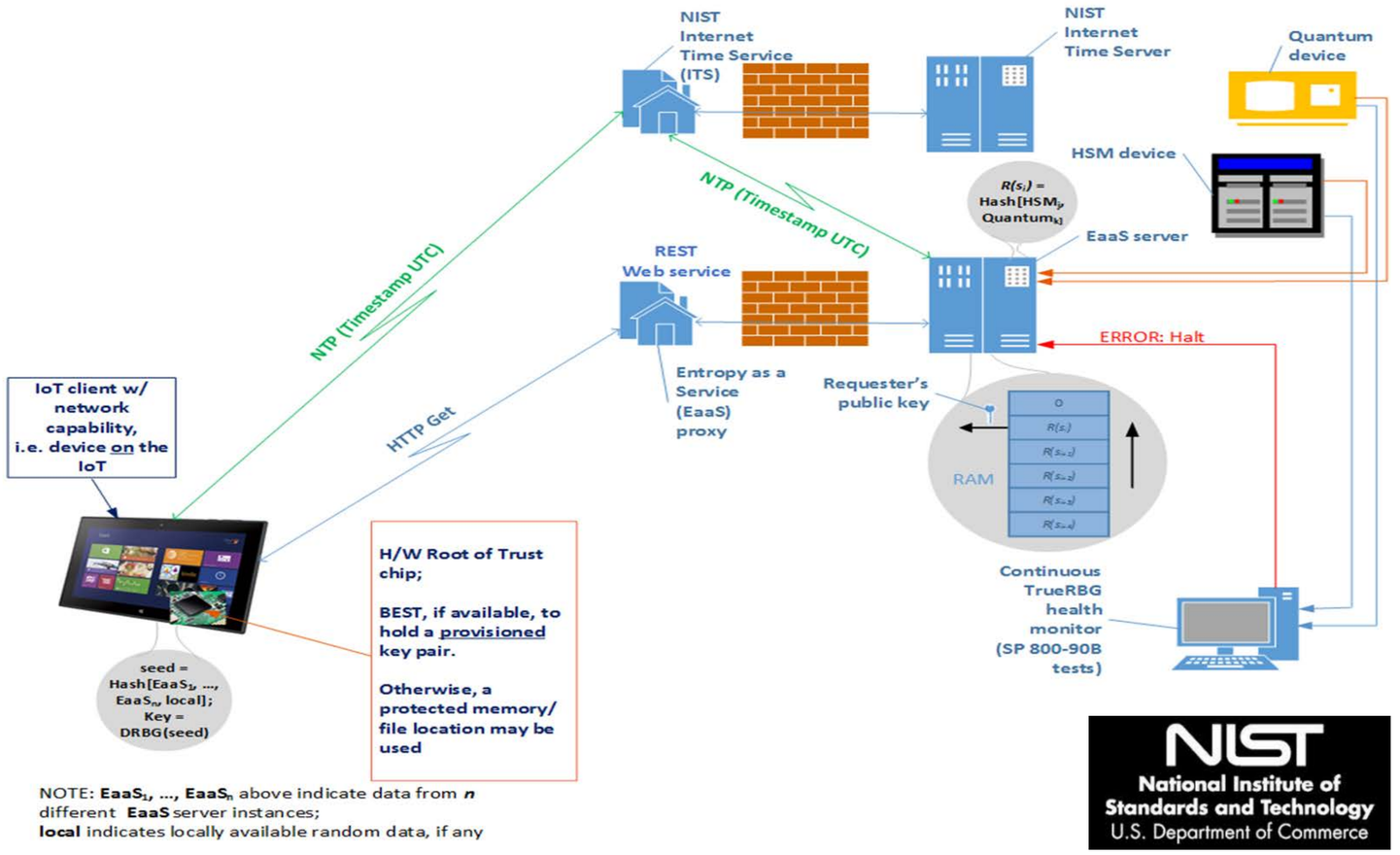
Entropy* as a Service

Kubernetes@Bare Metal

*Entropie ist in der Informationstheorie ein Maß für den mittleren Informationsgehalt einer Nachricht.



Das Zielbild der Cloud Stacks: Zentrales Management aller Sicherheits-domänen



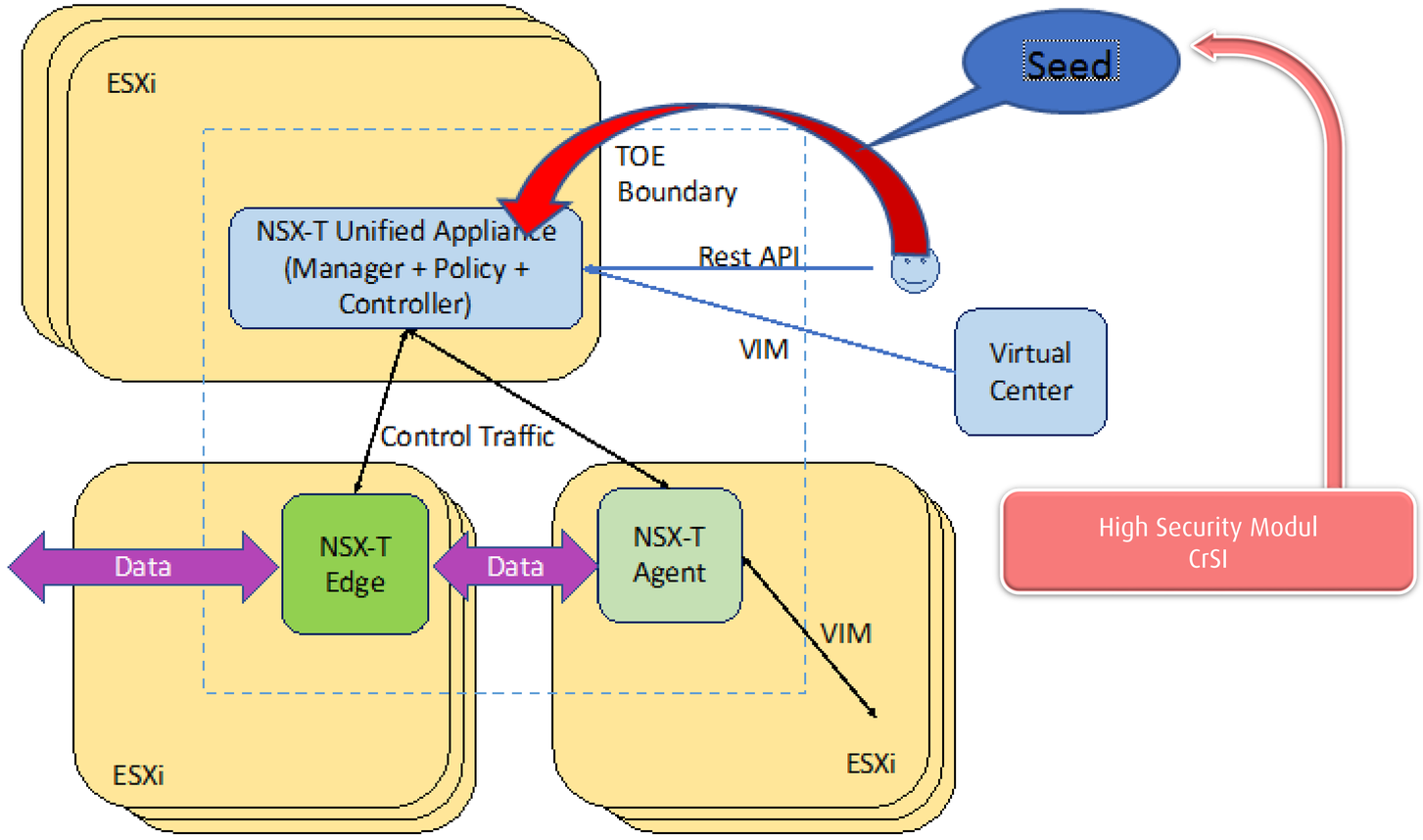
Grafiksprache: Bundeswehr

Um diesen Risiken begegnen zu können, bedarf es Sicherheit von außen durch **Entropy as a Service (Eaas)**

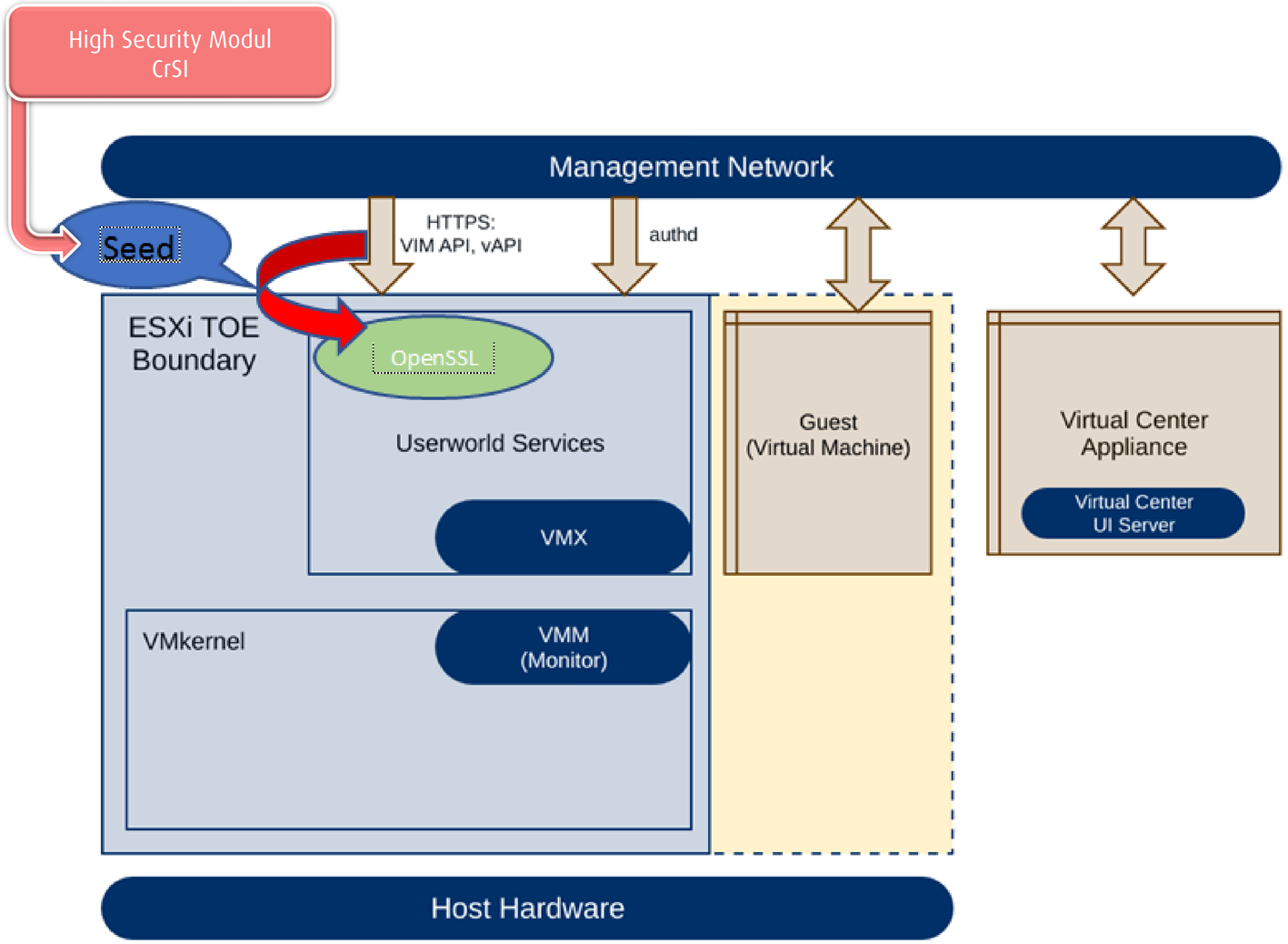
Vmware:A. Vassilev and R. Staples. "Entropy-as-a-Service: Unlocking the Full Potential of Cryptography". *IEEE Computer*. September 2016. – RSA Konferenz 2020

pCloudBw EaaS Proposal: Verschlüsselung von außen

Entropy Proposal – NSX-T Netzwerkebene



Grafiksprache: Bundeswehr



Grafiksprache: Bundeswehr

pCloudBw EaaS Proposal: Verschlüsselung von außen

Entropy Proposal – ESXi Virtualisierung Umgebung

Themen

Einsatzspektrum &
Aufbau der pCloudBw

Herausforderung durch
Quantencomputing

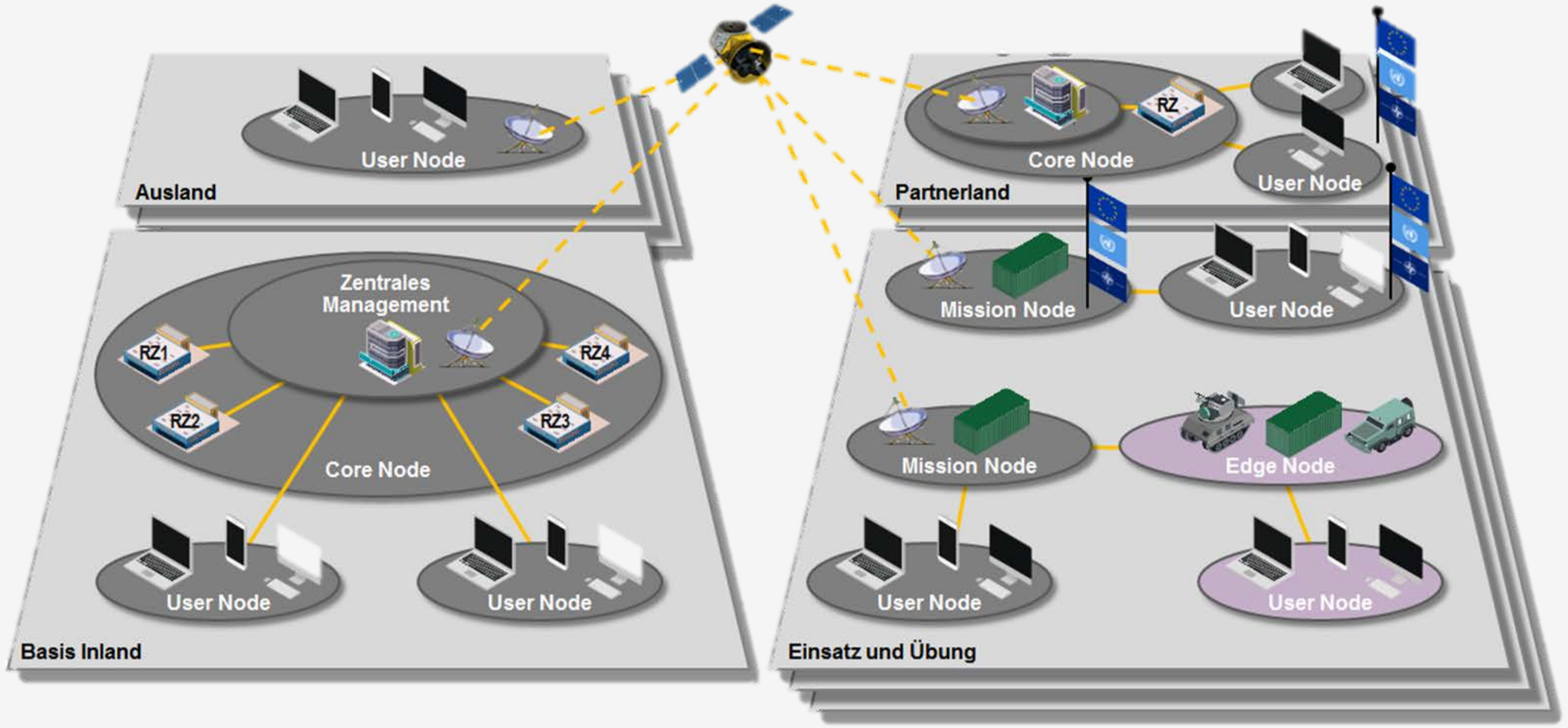
Entropy* as a Service

Kubernetes@Bare Metal

*Entropie ist in der Informationstheorie ein Maß für den mittleren Informationsgehalt einer Nachricht.

Bild Internet - mekongnet

Die Skalierung des pCloudBw Service auf Einsatzumgebungen stellt eine Herausforderung da

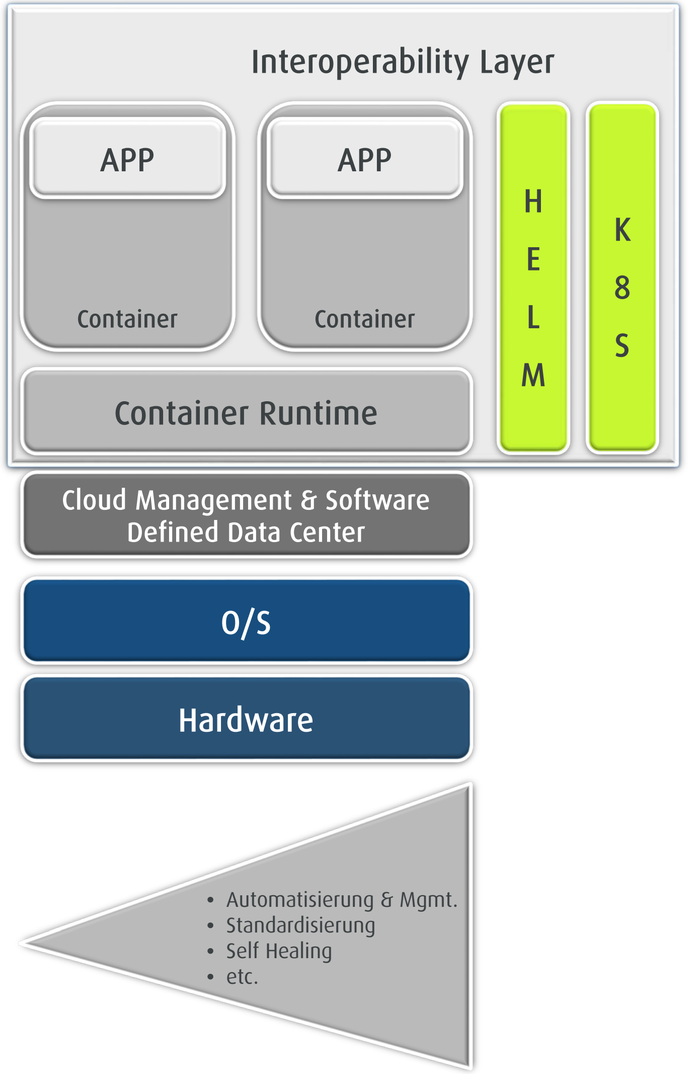


Grafiksprache: Bundeswehr

Kubernetes@BareMetal Kann dieser Herausforderung begegnen

- Vorteile:
- **Höhere Leistung** mit Einsatz von Systemressourcen für die Hardwareemulation
- Volle **Nutzung aller Maschinenressourcen**
- **Einfachere Administration**
- Größere **Performance** für Applikationen
- **Mobile Umgebungen** - mit Host-Server Wechsel
- Anwendungen erhalten **Zugriff auf Bare-Metal-Hardware** - ohne Pass-through-Techniken

- Herausforderungen:
- Geringerer Grad an **Isolierung**
- Implementierung benötigt **spezifisches OS** auf der Hw, welches selbst aufgebracht und gemanagt werden muss
- Übergreifendes separates **Sicherheits- und Betriebsmanagement notwendig**



Grafiksprache: Bundeswehr

Für die Begegnungen der Bedrohungen durch Quantenencomputing und der Umsetzung der pCloudBw auf Einsatzsystemen suchen wir Partner für..

...Ableitung & Umsetzung des Bare-Metal-Ansatzes

...die Umsetzung von Entropy-as-a-Service

...die Bereitstellung von Quantencomputing-Resistant Entropy

Wir freuen uns auf Ihre Kontaktaufnahme!

Markus Hauff

–

BWI GmbH, CDO
Digitale Programme STA
+49 2225 988 6915
Markus.Hauff@bwi.de

Bildquelle: BWI/Löschke