



Mehr Forschung wagen!

Forschen und Entwickeln für eine digitale
Souveränität in Europa

Brigadegeneral Jens-Olaf Koltermann

Jahrestagung CODE

München, den 12. Juli 2018



Mutige Wissenschaftler sind Treiber für Innovationen



***Der Fortschritt mag ja gut und schön sein,
aber er dauert zu lange.***

(Ogden Nash)

Stagnation ist der Anfang vom Ende.

(Sokrates)

***Das größte Hindernis für den wissenschaftlichen Fortschritt ist die
Weigerung einiger Leute, Wissenschaftler mit eingeschlossen, zu glauben,
dass unbegreiflich scheinende Dinge wirklich geschehen können.***

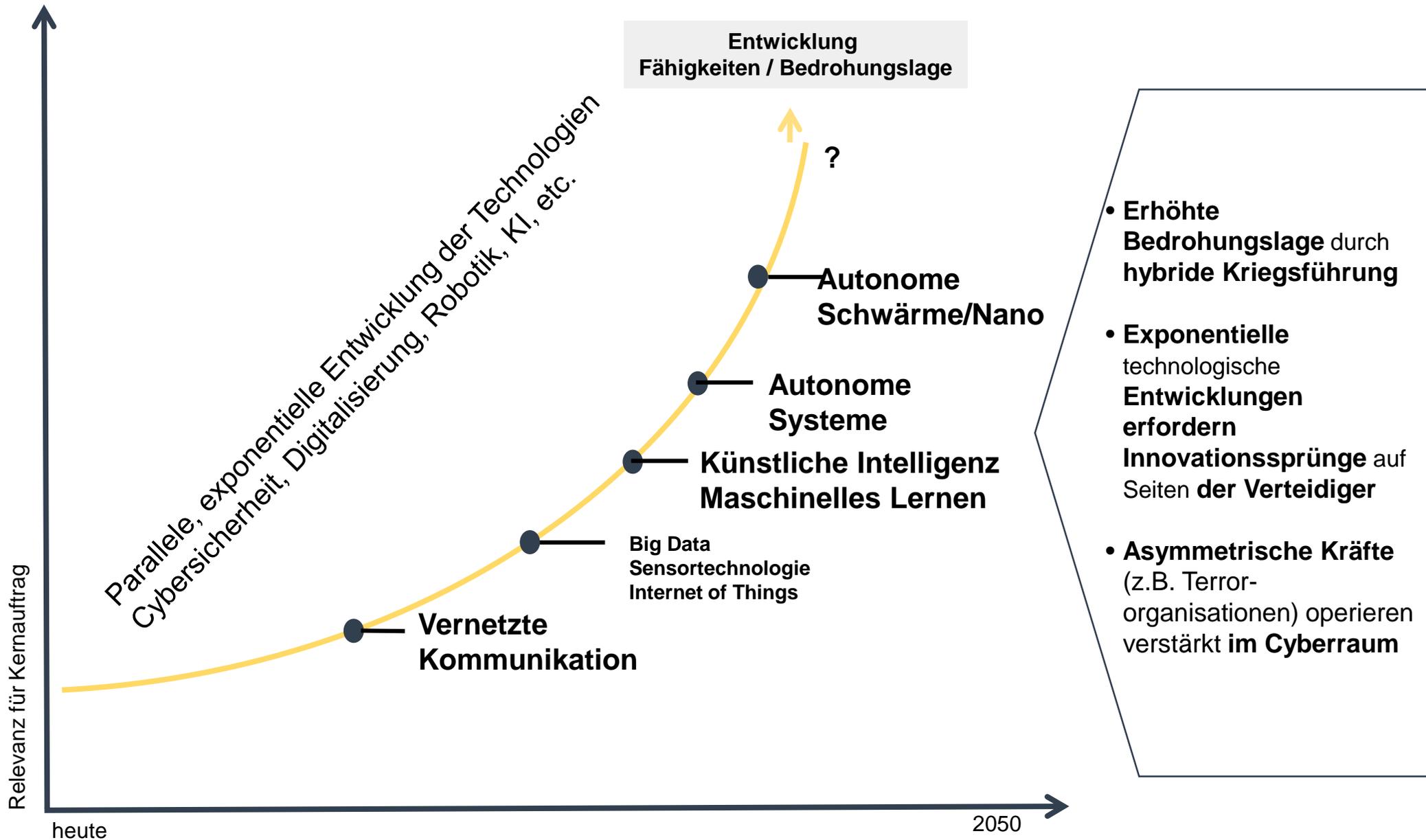
(George S. Trimble, Direktor des NASA-Spacecraft Center in Houston)

***Fortschritt ist nur möglich, wenn man
intelligent gegen die Regeln verstößt.***

(Boleslaw Barlog)



Die Bundeswehr muss mit der dynamischen Entwicklung im Cyberraum Schritt halten können



Technologischer Bedarf: Delta in Entwicklungsgeschwindigkeit muss geschlossen werden



Die Forschungsexpertise ist auf unseren Bedarf abgestimmt





Welchen Forschungsbedarf wir konkret haben





Der Forschungs- und Entwicklungsbedarf fokussiert auf unsere Bedarfe (1/2)



Anwendungsfeld

Cyber- verteidigung



Erlangen digitaler Souveränität durch Entwicklung von sicherer und vertrauenswürdiger Informationstechnologie (verteidigungsindustrielle Schlüsseltechnologien)

Ausbau der Schutzmöglichkeiten des IT-SysBw und der IT-Infrastruktur (durch starke Kryptografie-Verfahren)

Erhöhung der Resilienz eigener IT-Infrastruktur gegen elektromagnetische Einflüsse und Cyber-Angriffe

Schutz kritischer Informationsversorgungssysteme zur Sicherstellung eigener Führungsfähigkeit

Anwendungsfeld

Unbemannte Systeme



Entwicklung von Mensch-Maschine-Schnittstellen

Miniaturisierung von Sensortechnologie

Sicherstellung sowie Schutz robuster breitbandiger Kommunikationsverbindungen über große Distanzen



Der Forschungs- und Entwicklungsbedarf fokussiert auf unsere Bedarfe (2/2)



Weitere
Anwendungs-
felder



Erhöhung der Leistungsfähigkeit von Echtzeit-Computersystemen unter den Bedingungen von Interoperationalität in global verteilten IT-Architekturen durch künstliche Intelligenz

Ausbau und Weiterentwicklung der vernetzten Operationsführung

Digitalisierung der Verwaltung durch eAkte, elektronische Vorgangsbearbeitung sowie elektronische Zusammenarbeit



Forschung und Innovation sind Mosaiksteine für die Gewährleistung von Informationssicherheit



InfoSichh wird im Rahmen eines **Informationssicherheitsmanagementprozesses** erreicht durch

- Umsetzung, Gewährleistung und Überwachung von technischen Maßnahmen bzw. Maßnahmen an der IT selbst (**Technische InfoSichh**) sowie
- von personellen, infrastrukturellen und organisatorischen Maßnahmen im Einsatzumfeld der IT (**Sicheres IT-Umfeld**)

Steuerkreis Informationssicherheit
Ltg CISO Ressort

CISO Infrastruktur

- verantwortlich für die Umsetzung der Informationssicherheit in Infrastrukturen
- Liefert Beitrag InfoSichLage Infrastruktur

Inspektionen von Rüstungs- und Infrastrukturprojekten

stellen die Durchsetzung von Maßnahmen der Informationssicherheit sicher

CISO Rüstung

- verantwortlich für Umsetzung der Informationssicherheit in Rüstungsprojekten der Bw
- Liefert Beitrag InfoSichLage Rüstung

Penetrationstesting
um realitätsnah Schwachstellen zu identifizieren.

Prozess Informationssicherheit gewährleisten

systematisiert und verstetigt Aktivitäten der Informationssicherheitsorganisation und verknüpft sie mit den Leistungs- und Hauptprozessen der Bw und garantiert so ihre durchgängige Berücksichtigung

CODE UniBw M

entwickelt und schreibt fort die Technology Roadmap für Schlüsseltechnologien im Bereich InforSicherheit

Cyber Innovation Hub (CIH)

Aufnahme von Impulsen durch Start-Ups und Trends außerhalb der Bundeswehr

Security Lab UniBw M

entwickelt die Info-Sicherheit in technischer, organisatorischer und prozeduraler Hinsicht weiter

SIEMBw

überwacht und analysiert Sicherheitsereignisse 24/7 und leitet ggf. Maßnahmen ein



**Wir handeln nicht allein,
unsere Aktivitäten sind eingebettet !**



- Gesamtstaatliche Fähigkeiten ausbauen, also **ressortübergreifend kooperieren** und mit Wissenschaft, Industrie und Partnern **vernetzen**
- Eigene **Cyberfähigkeiten ausbauen**, dabei Sicherheitsarchitektur des IT-Systems der Bw konsolidieren und **resilienter** machen
- **Waffensysteme und Gefechtsstände** sowie Lieferketten in der Rüstung **härten**
- **Spitzenpersonal** durch Schaffung attraktiver Cyberkarrierepfade [...] **rekrutieren**
- Fragmentierte **Zuständigkeiten** und Strukturen für einen robusten Fähigkeitenaufbau **zusammenführen**, die **IT-Fähigkeiten bündeln** sowie zentrale Ansprechpartner für andere Ressorts und multinationale Partner schaffen



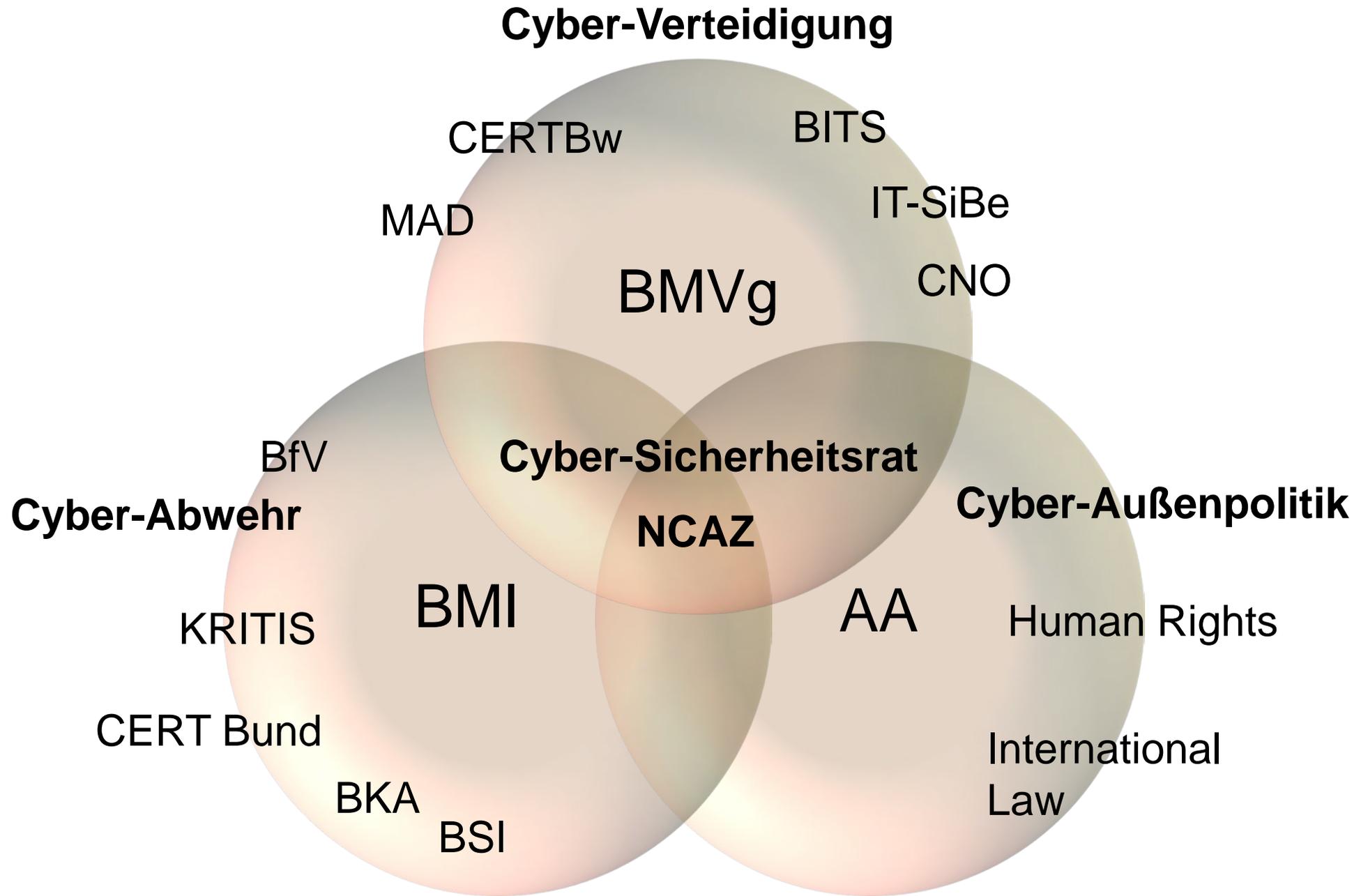
Cyber-Sicherheitsstrategie für Deutschland - bundeswehrspezifisch -



- Deutlich **stärkere Rolle der Bundeswehr** in der gesamtstaatlichen Sicherheitsvorsorge
- **Schutz Kritischer Infrastrukturen ressortgemeinsame Aufgabe**
- Auf- und Ausbau eines **Cyber-Cluster** bei UniBw M
- **Weiterentwicklung des NCAZ** mit engerer Bw- Beteiligung
- Bw **Incident Response Teams** Teil der gesamtstaatlichen Sicherheitsvorsorge (**Amtshilfe**)
- Intensivierung der **Zusammenarbeit nationaler CERT** Strukturen
- Aufbau einer **Cyber-Reserve** in der Bw
- Cyber-Raum ist **Operationsraum** (analog NATO)



Cyber-Sicherheitsarchitektur





Digitale Souveränität

Wir forschen auf internationalem Niveau und erschließen
uns Schlüsseltechnologien.

Wir stärken Experten-Systeme und
entscheiden selbst was wir tun.



Mehr Forschung wagen!

Forschen und Entwickeln für eine digitale
Souveränität in Europa

Brigadegeneral Jens-Olaf Koltermann

Jahrestagung CODE

München, den 12. Juli 2018