NEWSLETTER VERTEIDIGUNG

04. AUGUST 2020 I ISSN 2194-0088 I 12. JAHRGANG

AUSGABE 31

# Cyber-Kooperation zwischen Deutschland und den USA wird intensiviert

# Intensivierung der deutsch-amerikanischen Kooperation im Bereich Cyber und Informationstechnik

*Von OTL i.G. Stefan Eisinger*

***Sowohl Deutschland als auch die Vereinigten Staaten von Amerika sehen sich seit dem Ende des Kalten Krieges einem vielfältigeren und komplexeren Sicherheitsumfeld gegenüber. Die Informationstechnik und die Nutzung des Cyberraumes bieten Nationen beispiellose Chancen, bergen jedoch auch Risiken. Die daraus resultierenden Herausforderungen für Sicherheit und Stabilität können für unsere Gesellschaften, Volkswirtschaften und Institutionen ebenso schädlich sein, wie konventionelle Angriffe.***

Auf dem NATO-Gipfel in Wales im September 2014 haben die Staats- und Regierungschefs beschlossen, dass "Cyber Defense" eine der Kernaufgaben der NATO im Rahmen der Bündnisverteidigung ist. Sie bekräftigten das Verteidigungsmandat der NATO im Juli 2016 auf dem Warschauer NATO-Gipfel und versprachen, ihre nationalen Netzwerke und Infrastrukturen besser gegen Angriffe aus dem Cyberraum zu schützen – auch bekannt als Cyber-Defense-Pledge – und erkannten den Cyberraum als eine weitere Dimension militärischer Operationsführung an.

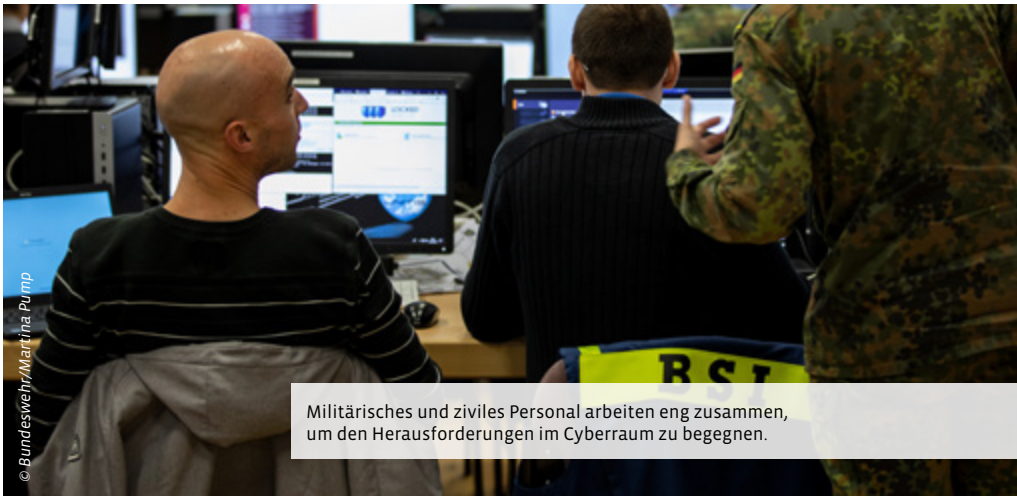
Der Cyberraum ist ein von Menschen erschaffenes Konstrukt, das einer stetigen Weiterentwicklung unterliegt. Es unterscheidet sich damit deutlich von den traditionellen Dimensionen militärischer Operationsführung. Akteure mit feindseligen Absichten können sich zu relativ geringen Kosten und teilweise mit einfach verfügbaren Hilfsmitteln Zugang zu Fertigkeiten, Fähigkeiten und Ressourcen verschaffen, die benötigt werden, um im und durch den Cyberraum disruptive Aktivitäten zu entfalten. Um die beabsichtigte Wirkung zu erzielen, können Angreifer hierbei auch fortschrittliche Technologien anwenden, gegebenenfalls in Verbindung mit traditionellen militärischen und diplomatischen Maßnahmen. Die Möglichkeit, Daten und Informationen über den Cyberraum zu manipulieren, bietet Angreifern die Chance, angestrebte Effekte schnell zu realisieren. Eine technische Rückverfolgbarkeit wird dabei gezielt erschwert.

In Deutschland spricht man vom Cyber- und Informationsraum (CIR) als Dimension der militärischen Operationsführung und fasst somit die Definition weiter und umfassender als die NATO, Alliierte und internationale Partner. Der CIR ist der erschließbare, zugleich virtuelle, physische und kognitive Raum, der aus dem Cyberraum, dem elektromagnetischen Umfeld sowie dem Informationsumfeld besteht.

### *Herausforderungen im Cyberraum erfordern einen gut koordinierten multinationalen Ansatz*

Angesichts des komplexen und vielfältigen Charakters des Cyberraumes ist es wichtig zu verstehen, dass keine Nation oder Institution allein über alle notwendigen Kenntnisse, Fähigkeiten, Kapazitäten und Befugnisse verfügt, um ihre Interessen im und durch den Cyberraum adäquat zu sichern.

Die Verbesserung der Sicherheit, die Erhöhung der Widerstandsfähigkeit und die Nutzung von Potenzialen im Cyberraum erfordern eine breit angelegte, streitkräftegemeinsame, multinationale und behördenübergreifende Koordination erforderlich. Diese sollte insbesondere den zivilen Sektor mit Wissenschaft, Industrie und zivilgesellschaftliche Organisationen berücksichtigen und einschließen.

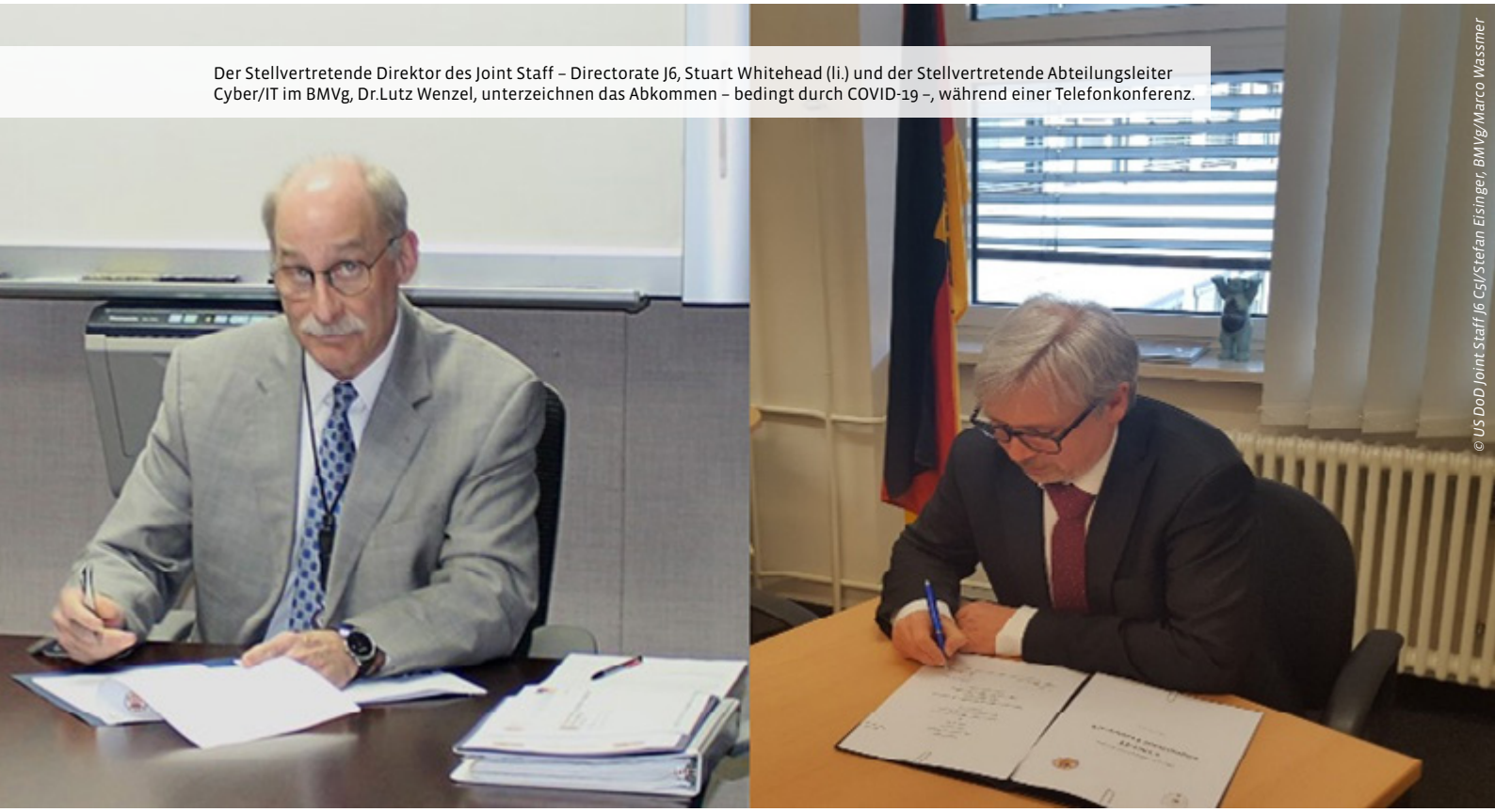



© Bundeswehr/Martina Pump

Militärisches und ziviles Personal arbeiten eng zusammen, um den Herausforderungen im Cyberraum zu begegnen.

Demnach ist es entscheidend, sachkundige Partner und Verbündete zu finden, um den Herausforderungen im Cyberraum entschlossen begegnen zu können. Beziehungen zwischen Nationen aufzubauen, die bereit sind, maßgeblich in militärische Fähigkeiten im Cyberraum zu investieren, ist keine leichte Aufgabe. Diese engen Beziehungen nachhaltig zu pflegen und zu fördern gestaltet sich oftmals sogar noch anspruchsvoller.

Ende 2019 sind Deutschland und die USA darin übereingekommen, ihre Kooperation in den Bereichen Cyber und IT zu intensivieren. In der ersten Jahreshälfte 2020 wurde zwischen beiden Staaten auf ministerieller Ebene eine bilaterale Vereinbarung, Cyber/IT Engagement Framework (CITEF), zwischen dem Stellvertretenden Direktor C5I, US Joint Staff J6 und dem Stellvertretenden Abteilungsleiter Cyber/Informationstechnik im Bundesministerium der Verteidigung gezeichnet. Insbesondere die Initiative eines Verbindungsoffiziers des Planungsamtes der Bundeswehr beim US Joint Staff J6 machte diesen schnellen Erfolg möglich.



Der Stellvertretende Direktor des Joint Staff – Directorate J6, Stuart Whitehead (li.) und der Stellvertretende Abteilungsleiter Cyber/IT im BMVg, Dr.Lutz Wenzel, unterzeichnen das Abkommen – bedingt durch COVID-19 –, während einer Telefonkonferenz.



Diese Vereinbarung konkretisiert die Bereiche der künftigen Kooperation zwischen dem US Joint Staff J6 und der Abteilung Cyber/ Informationstechnik des BMVg.

Es werden Aspekte in den Bereichen IT-Governance/IT-Management, IT-Ausbildung und IT-Übungen sowie der IT-Fähigkeitsentwicklung adressiert.

***Verbesserung der Interoperabilität und Vertrauensbildung***

Das Multinational Interoperability Council formuliert hierzu: „the future coalition operational environment must be one in which interoperability has been contemplated and addressed well in advance“ (s. MIC, Coalition Building Guide (CBG) Band III.1, Version 4.1, November 2012, S. 3).

Das übergeordnete Ziel des bilateralen Cyber/IT Engagement Framework (CITEF) ist es, die Interoperabilität der Streitkräfte sowie das Vertrauen zwischen den deutschen und amerikanischen Streitkräften zu stärken.

Das Multinational Interoperability Council (MIC) wurde im Oktober 1996 aufgestellt. Es dient der Kontrolle der Interoperabilität von Koalitionen und soll bei deren Bildung Unterstützung leisten. Am 30. August 2019 wurde das MIC in Multinational Strategy and Operations Group (MSOG) umbenannt.

Die NATO definiert Interoperabilität von Streitkräften als „the ability of the forces of two or more nations to train, exercise and operate effectively together in the execution of assigned missions and tasks." Allgemeiner formuliert: „Interoperability is the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives" (vgl. NATO Glossary of Terms and Definitions (AAP-06), Edition 2019).

Folglich kann sich die Interoperabilität der Streitkräfte nicht nur auf technische Fragen beschränken. Grundsätze, Doktrinen, Verfahren, kulturelle Aspekte und sogar die Sprache spielen eine wichtige Rolle um die Interoperabilität von Streitkräften zu entwickeln, zu erhöhen und aufrechtzuerhalten. Um dieser Tatsache Rechnung zu tragen, umfasst das deutsch-amerikanische Cyber/IT Engagement Framework bilaterale Maßnahmen in einem breiten Spektrum unterschiedlicher Aspekte von Interoperabilität. Es konkretisiert Maßnahmen, die sich von militärischer Fachausbildung und Übung bis hin zur gemeinsamen Erarbeitung von Regelwerken sowie der Abstimmung detaillierter technischer Spezifikationen erstrecken. CITEF hat ein Umfeld geschaffen, in dem deutsche und amerikanische Experten offen miteinander diskutieren und koordiniert Informationen austauschen können. Absicht ist es, wesentlich zu den laufenden Bemühungen um Vertrauensbildung beizutragen und dadurch auch die Effizienz und Effektivität multinational geführter Einsätze positiv zu beeinflussen. Das CITEF schafft letztlich die Grundlage dafür starke, nachhaltige Arbeitsbeziehungen zu entwickeln, Reibungsverluste zu verringern und den militärischen Erfolg zu gewährleisten.

***Positiver Effekt für Federated Mission Networking und die Arbeit der NATO***

In vielen Aspekten der Interoperabilität und der multinationalen Nutzung des Cyberraumes sind die NATO und das Federated Mission Networking (FMN), eine von der NATO unterstützte Initiative, wesentliche Treiber. Diese fokussieren sich vor allem darauf Grundsätze, Doktrinen, Verfahren und Standards im militärischen Kontext zu entwickeln.

***Federated Mission Networking***

"Federated Mission Networking is a capability aiming to support command and control and de-cision-making in future operations through im-proved information-sharing. It provides the agili-ty, flexibility and scalability needed to manage the emerging requirements of any mission envi-ronment in future military operations. Federated Mission Networking is based on principles that include cost effectiveness and maximum reuse of existing standards and capabilities" (vgl. NATO ACT, FMN Fact Sheet 2019).

Jährliche Übungen und Ereignisse wie die Coalition Warrior Interoperability Exercise (CWIX) und die Cyber Coalition konkretisieren diese Bemühungen und bieten die Möglichkeit Ansätze zur Bewältigung komplexer Herausforderungen im Cyberraum weiterzuentwickeln. Die bilateralen Bestrebungen zwischen Deutschland und den USA zielen in erster Linie darauf ab, die Interoperabilität nachhaltig zu verbessern und dies durch die Förderung von NATO- bzw. FMN-Aktivitäten zu erreichen. Die Ergebnisse einzelner Kooperationsmaßnahmen werden nach ihrer Freigabe stets an die fachlich zuständigen NATO- bzw. FMN-Gremien weitergegeben.


Die Interoperabilitätsübung CIWIX (hier Impressionen aus Juni 2020) bietet einzigartige Möglichkeiten, die NATO-Zusammenarbeit auf IT-Ebene zu trainieren.

Fotos: © NATO

Ziel ist es, durch den kontinuierlichen Austausch von Erkenntnissen, die laufenden Arbeiten zur Verbesserung der Interoperabilität gegenseitig zu befördern und ggf. weitere koalitionsgeführte Aktivitäten anzustoßen. Zudem sollen mit den bilateralen Cyber-/IT-Kooperationsaktivitäten zwischen Deutschland und den USA ehemals isolierte nationale Ansätze besser synchronisiert, harmonisiert und koordiniert werden, um dadurch ebenfalls positive Effekte in der NATO bzw. dem FMN zu erzielen.

### *Das Cyber/IT Engagement Framework*

Im bilateralen deutsch-amerikanischen Cyber/IT Engagement Framework werden in einem Zwei-Jahres-Rhythmus angestrebte Ziele (Desired Outcomes) auf ministerieller Ebene definiert und abgestimmt. Das CITEF dient somit als wesentliche Orientierungshilfe, um detaillierte bilaterale Maßnahmen zu entwickeln. Im Anhang zum CITEF werden für jedes angestrebte Ziel sogenannte Operationslinien (Lines of Effort) festgelegt. Innerhalb jeder Operationslinie werden konkrete Kooperationsaktivitäten mit klaren Zeitlinien definiert. Diesem Grundsatz folgend kann jede bilaterale Maßnahme, die im Rahmen des CITEF durchgeführt wird, letztlich auf die zuvor festgelegte Absicht der übergeordneten Führung nachverfolgt werden. Darüber hinaus ermöglichen spezifische Arbeitspläne die verfügbaren Ressourcen für jede Maßnahme effektiv und effizient zu nutzen. Das CITEF, einschließlich seines Anhangs, wird regelmäßig fortgeschrieben.

## Desired Outcomes (DO)

***DO 1: "IT-Management/IT-Governance"***

Align USA and DEU Service Management and Control (SMC) capabilities within the Federated Mission Networking (FMN) IOT enable "Day Zero Interoperability" in IT/SMC operations and inform NATO and/or Federat-ed Mission Networking (FMN) activities. Exchange IT-Governance doctrines, concepts, policies and ideas to increase mutual understanding and inform national doctrinal work.

***DO 2: "IT Training and Exercise"***

Participate in/contribute to mutual IT training and exercise events IOT ensure "Day Zero Interoperability" by increasing understanding in planning, joining, executing, and exiting mission networks in a multinational envi-ronment. Share training and exercise burdens and align efforts. Bilateral TREX activities complement and leverage NATO-driven activities. Attend mutual Professional Military Education (PME) events related to Cyber and IT.

***DO 3: "IT Capability Development"***

Institutionalize the exchange of information, expertise and knowledge of IT requirements and projects IOT facilitate IT requirements and capability development. The USA and DEU are Affiliates within the NATO Initia-tive Federated Mission Networking. The aim is to enhance Day Zero interoperability between NATO, NATO nations and non NATO Nations and entities. Primary focus based on FMN efforts is on the Mission Partner Environment (MPE), German Mission Network (GMN), IT-Service Management Platform and Military Cloud efforts. Secondary focus is to align IT requirements development, where FMN spirals specifications provide a "pacing mechanism".

Quelle: CITEF – Desired Outcomes (Originaltext)

***Vision und Zukunftsperspektive***

Das CITEF ist seit Jahrzehnten das erste von Deutschland und den USA unterzeichnete Abkommen zur konkreten Zusammenarbeit im Bereich Cyber/IT. Es gilt als erster Schritt zu einer intensiveren Kooperation zwischen den Vereinigten Staaten von Amerika und Deutschland. Ausgehend von den Erfahrungen, die beide Nationen mit den koordinierten Kooperationsaktivitäten gewinnen werden, wird das CITEF im Laufe der Zeit überarbeitet und zunehmend reifen.

Das CITEF hat das Potenzial, einen strukturierten Dialog über die Herausforderungen und Chancen im Cyberraum auf oberster Führungsebene weiter zu konkretisieren sowie die Zusammenarbeit auf operativer und taktischer Ebene nachhaltig zu vertiefen.

Die Vereinbarung und ihre ersten Ergebnisse werden bei einem für Ende des Jahres 2020 geplanten Treffen im Pentagon zwischen dem Abteilungsleiter Cyber/Informationstechnik im BMVg, dem Direktor des US Joint Staff J6 und dem US DoD CIO Gegenstand weiterer Gespräche sein.

# 3 FRAGEN AN ...

## Herrn Generalleutnant Michael Vetter, Abteilungsleiter Cyber/Informationstechnik und CIO im Geschäftsbereich BMVg

© Josephine Klingner

## Fragen zum deutsch-amerikanischen Cyber/IT Engagement

***Die NATO hat den „Cyberspace" als wichtige militärische Dimension der militärischen Operationsführung identifiziert. Deutschland und die USA sind NATO-Partner. Warum eine vertiefte bilaterale Zusammenarbeit?***

**Vetter:** Die Vereinigten Staaten und Deutschland arbeiten als enge Partner und Verbündete traditionell intensiv und vertrauensvoll zusammen. Darüber hinaus eint uns wie in kaum einer anderen Dimension, trotz geografischer Trennung, der „gemeinsame Cyberspace". Die Vertiefung der Beziehungen in diesem immer bedeutender werdenden Bereich „Cyberspace" ist also nicht nur logisch, sondern auch zwingend. Die USA und Deutschland verbindet ein gemeinsames Verständnis des Cyber- und Informationsraums als Dimension militärischer Operationsführung. Die gemeinsame Arbeit unter dem Dach des CITEF ermöglicht es den USA und Deutschland im Schulterschluss wichtige Impulse im Bündnis zu setzen. Deutschland wiederum vermag auf diese Weise auch eine europäische Perspektive in die USA zu transportieren; umgekehrt kann die USA Position auch im Europäischen Kontext Berücksichtigung finden. Wir können zu beiderseitigem Nutzen voneinander lernen und diese Erkenntnisse dann mit anderen Partnern und Verbündeten teilen.

***Die Abteilung CIT und das Kommando CIR sind relativ „junge“ Organisationen. Sind die Arbeitsabläufe, Verfahren und Beziehungen schon „reif“ für die bilaterale Kooperation mit dem wichtigsten Bündnispartner?***

**Vetter:** Deutschland ist in der NATO fest verankert. Ein nationaler militärischer Alleingang kommt überhaupt nicht in Betracht. Die Bundeswehr verfügt über jahrzehntelange, gefestigte Erfahrung in der bi- und multinationalen Kooperation. Dies gilt in besondere Weise auch für die Zusammenarbeit mit unseren amerikanischen Freunden. Die internationale Vernetzung war auch ein konstitutives Merkmal bei der Aufstellung des militärischen Organisationsbereichs Cyber- und Informationsraum. So wurde beispielsweise der Anteil „internationale Kooperation“ im Kommando CIR schon mit Aufstellung des Kommandos direkt dem Chef des Stabes zugeordnet. Die internationalen Kontakte, insbesondere zu den US-Stellen, wurden bereits durch den „Aufbaustab Cyber“ im BMVg etabliert und anschließend durch das Kommando CIR weiter verstetigt. In der Abteilung CIT ist der Anteil Internationale Kooperation im Referat für Cyberpolitik verortet und hat bestehende internationale Arbeitsbeziehungen der ehemaligen Abteilung AIN fortgesetzt und ausgeweitet. Es ist so gelungen, von Beginn an, ein Netzwerk mit unseren Partnern und Alliierten – allen voran mit den USA – zu etablieren, das wir gezielt weiter ausbauen und vertiefen.

***Die Weiterentwicklung von Fähigkeiten staatlicher und nichtstaatlicher Akteure findet vor allem außerhalb der Streitkräfte statt. Ist die Bundeswehr technisch in der Lage, „mitzuhalten“?***

**Vetter:** Die Bundeswehr ist modern ausgestattet und verfügt über hervorragend ausgebildetes und motiviertes Personal. Dies gilt ausdrücklich auch für den Bereich CIR. Wir investieren hier gezielt in neue Fähigkeiten. So wurden das Zentrum für Cybersicherheit der Bundeswehr und das Zentrum für Softwarekompetenz der Bundeswehr neu aufgestellt; das Zentrum Cyberoperationen wurde personell verstärkt. Um das hierfür notwendige qualifizierte Personal zu gewinnen und zu binden, haben wir eine Vielzahl von Maßnahmen gestartet. Diese beinhalten beispielsweise ein Masterstudium Cybersicherheit, die Einführung einer Fachkarriere für ausgewählte Offiziere, die Gewährung von Zulagen für Cyber- und IT-Spezialisten und den Aufbau einer Cyber Reserve. Um mit der Dynamik des zivilen Sektors auch in materieller Hinsicht Schritt halten zu können, investieren wir gezielt in Innovationen und Agilität. Der Cyber Innovation Hub der Bundeswehr als Schnittstelle in die Start-Up-Welt, das Forschungsinstitut CODE („Cyber Defence und Smart Data“) an der Universität der Bundeswehr in München und die jüngst gegründete Agentur für Innovation in der Cybersicherheit sind „Leuchttürme“ in diesem Bereich. Im Zuge des Konjunkturpaketes stehen uns Haushaltsmittel in Höhe von bis zu 500 Mio € zur Verfügung, um mittels eines Zentrums für Digitalisierungs- und Technologieförderung die Forschung an den Universitäten der Bundeswehr in allen Bereichen nationaler Schlüsseltechnologien zu fördern.