Positionspapier

AK Verteidigung: Neuorganisation des Cyber- und Informationsraums im BMVg und im nachgeordneten Bereich

22. Februar 2016

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Marc Bachmann
Bereichsleiter Luftfahrt und Verteidigung
T +49 30 27576-102
m.bachmann@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Am 17.09.2015 hat das BMVg im Rahmen der Veranstaltung „Perspektiven Cybersicherheit“ und im Rahmen eines Tagesbefehls der Ministerin bekannt gegeben, dass nachhaltige Veränderungen im Bereich des Cyber- und Informationsraums beabsichtigt sind. Bitkom hat wiederholt Vorschläge gemacht, wie solche Veränderungen sowohl organisatorisch wie auch inhaltlich aussehen können.

Das vorliegende Positionspapier greift zahlreiche dieser Vorschläge auf und stellt 9 Thesen auf. Die folgend ausgeführten Punkte sind in Teilen bereits seit Jahren in der Diskussion und somit auch teilweise im Ministerium und nachgeordneten Bereich (Planungsamt, BAAINBw, BWI) bekannt: Es fehlte allerdings generell eine übergeordnete steuernde Kompetenz, die gegenüber allen Dienststellen der Bundeswehr weisungsbefugt ist und eine nachhaltige Veränderung übergreifend umsetzt.

1. **Die Bundeswehr muss sich auf die digitale Transformation einstellen und die Chancen zu ihrem Vorteil nutzen.**

Die digitale Transformation ist eine Revolution der Wirtschaft, aber auch von Gesellschaft und Verwaltung. Durch sie werden sich ganze Branchen, ganze Lebensbereiche grundsätzlich verändern - durch intelligente Fertigung in der Industrie 4.0, durch autonomes Fahren in intelligenten Verkehrsnetzen, durch eine massive Absenkung des Energieverbrauchs dank Smart Grids, durch eine Share Economy, die auf Nutzen statt auf Besitz gründet. Es entstehen komplett neue Geschäftsmodelle und Plattformen, die herkömmliche Bereiche transformieren. Das größte Taxiunternehmen der Welt besitzt keine Taxis, das größte Übernachtungsportal besitzt keine eigenen Hotelbetten, das größte Medienunternehmen besitzt keine eigenen Inhalte, der größte Retailer besitzt kein eigenes Inventar. Daneben ermöglichen neue Technologien wie 3D-Druck oder Virtualisierung ganz neue Möglichkeiten im Bereich Effektivität und Dynamisierung.
Auf die Bundeswehr übertragen bedeutet dies, dass sich die Art und Weise wie Kommunikation, Vernetzung, Verteidigung und Einsatzführung in Zukunft funktionieren, grundlegend verändern werden. Diese Herausforderungen sind aber auch zugleich Chancen. Die Frage ist vielmehr, wie sich die Bundeswehr auf die digitale Transformation einstellt und diese Herausforderungen zu ihren Gunsten annimmt. Sich hier nachhaltig und zukunftsfest aufzustellen, kann ein echter kompetitiver Vorteil sein. Die Möglichkeiten, die sich für die Bundeswehr ergeben sind mannigfaltig: Herstellung von Ersatzteilen direkt im Einsatzgebiet durch 3D-Druck, Datenerfassung und –analyse zur Informationsgewinnung, Big Data Lösungen für Logistik und Instandsetzung, moderne Lagebilderstellung für das vernetzte Gefechtsfeld, effizienterer Personaleinsatz in Waffensystemen (z.B. Fregatten oder Panzern) und vieles andere mehr. In Anbetracht der immer komplexeren Anforderungen an das Personal hinsichtlich Bedienbarkeit und Dynamik müssen unbedingt Normierungen, die aus dem IT-Weltmarkt abgeleitet werden können, in das Anforderungsmanagement für die IT in Waffensystemen einfließen und auch ergonomische Gesichtspunkte berücksichtig werden.
Das stellt natürlich auch deutlich erhöhte Anforderungen an die Sicherheit. Wenn alles stärker miteinander vernetzt ist, dann ergeben sich auch mehr Angriffspunkte. Deshalb ist es wichtig, dass IT-Sicherheit sowie Datenschutz schon von vornherein mitgedacht, konzeptionell berücksichtigt und implementiert werden (siehe dazu auch These 7).

2. **Die Bundeswehr muss neue Möglichkeiten der Zusammenarbeit mit der Wirtschaft finden, um im Bereich Innovationen nicht zurück zu fallen.**

Bitkom regt an, sogenannte Hubs für die Leitbranchen der deutschen und europäischen Wirtschaft wie Automobil, Logistik oder Pharmazie, aber auch Banken und Versicherungen zu schaffen.[1] In diesen Hubs oder Ökosystemen sollen die Flaggschiffe der jeweiligen Branche gemeinsam mit Mittelständlern und innovativen Start-ups, Hochschulen und Forschungseinrichtungen ein leistungsstarkes digitales Ökosystem bilden. Auf die Bundeswehr bezogen bedeutet das, dass neue Modelle der Zusammenarbeit gefunden werden müssen, die es der Bundeswehr ermöglichen innovative Lösungen nutzbar zu machen. Die Bundeswehr sollte die Bildung eines solchen Ökosystems nach ihren Bedürfnissen vorantreiben. In diesem Ökosystem, das sich über verschiedene Phasen (Plan – Build – Run), verschiedene Sicherheits-Dimensionen (Vertraulichkeit, Integrität, Authentizität sowie Verfügbarkeit und Resilienz), die unterschiedlichen Themenkomplexe der Technologie und Verfahren (z.B. Krypto, Endgeräte, Netze, Kommunikationsdienste wie E-Mail, Anwendungsdienste aber auch hybride IT-Infrastrukturen), verschiedene Zonen der IT-Sicherheit im Sinne

[1] Siehe Bitkom Hubs Konzept.

Absicherungsniveau, und verschiedene Formen der Leistungserbringung (Orchestrated Managed Services) erstreckt, können verschiedenste Kooperationsmodelle praktiziert werden – vom informellen Best Practice Sharing bis hin zu kreativen Modellen zur Unterstützung im operativen Betrieb, beispielsweise der Bereitstellung von gemanagten IT- und Unterstützungsdiensten, Cloud-Diensten oder komplettes Outsourcing. Determiniert durch das Level of Ambition sind hier neben der notwendigen Effektivität (Wirkung) auch die Effizienz (Wirtschaftlichkeit) verhältnismäßig abzubilden. In diesem Rahmen ist ein effektives Innovationsmanagement möglich.

3. Die Bundeswehr kann mit der Stärkung des Bereichs Cyber zur Digitalen Souveränität Deutschlands beitragen

Eine Stärkung des Bereichs Cyber kann zu einer größeren Digitalen Souveränität führen, die Bundeswehr kann hier eine sehr wichtige Rolle einnehmen. Digital souveräne Systeme können für sich beurteilen, welche Schlüsseltechnologien in einer digitalen Welt erforderlich sind und wie sie diese Schlüsseltechnologien aufbauen bzw. weiterentwickeln können, um hier selbstbestimmt agieren zu können. Als digitale Schlüsseltechnologien und -kompetenzen begreifen wir insbesondere

- Entwicklungs- und Produktionskompetenzen rund um IT-, Netzwerk- und Plattformsicherheit,
- Kompetenzen, digitale Technologien, Lösungen und Plattformen zu verstehen, zu prüfen, sowie intelligent und verantwortungsvoll für die Weiterentwicklung der eigenen Geschäftsmodelle einzusetzen und
- sie entsprechend dem Bedarfsfall so zu veredeln und zu härten, dass sie den jeweils angestrebten Sicherheitsanforderungen entsprechen.

Als digital souveränes System kann die Bundeswehr eine Vorreiterrolle übernehmen. Verstärkt wird dies weiter, wenn die Bundeswehr ihre Fähigkeiten um IT-Sicherheit und IT-Sicherheitsprodukte EU- und NATO-weit anbietet und damit einen wesentlichen Beitrag für multinationale Zusammenarbeit leistet.

4. Das Verteidigungsressort muss einen CIO etablieren, der nachhaltig handlungsfähig ist.

Bitkom sieht die Notwendigkeit, dass für das gesamte Ressort der Bundeswehr eine einheitliche und durchgängige IT durchgesetzt und zentral gesteuert werden muss. Dies beginnt bei einer einheitlichen Architektur, geht über eine zentrale Beschaffung und erstreckt sich über alle Fähigkeitskategorien. Dies kann ggf. auch in einer verteilten Organisationsform erfolgen. Ziel muss generell aber sein, dass der IT-Bereich (und zwar insbesondere in Person des CIO) handlungsfähiger wird. Im Sinne einer einheitlichen Architektur muss der CIO eine diesbezügliche planerische und haushalterische Eigenständigkeit erhalten. Zusätzlich erfordert dies einen deutlichen Kompetenzaufbau (im Stab/nachgeordneten Bereich) und die Erteilung von Weisungsbefugnissen inklusive Mitsprache- und Vetorecht. Dies muss durchgehend in der gesamten Organisationstruktur geregelt werden. IT kann i.d.R. nicht beschafft werden wie „traditionelle“ Rüstungsprojekte. Deshalb müssen sowohl die Beschaffungsprozesse als auch die Vertrags-bedingungen den kurzen Innovationszyklen Rechnung tragen und dementsprechend angepasst werden. Da IT immer auch querschnittlich gedacht werden muss, ist es notwendig, die entsprechenden organisatorischen, aber auch die technischen Schnittstellen zu definieren und einheitliche IT-Lösungen auch in unterschiedlichen Systemen zu verankern. Ansonsten wird der IT-Bereich nur ein weiteres Silo werden und eine effektive und effiziente Rüstung in Gänze (d.h. über alle OrgBereiche hinweg) nahezu unmöglich machen. Das Insourcing der BWI zum Jahresende 2016 eröffnet hier zudem neue Möglichkeiten. Die BWI sollte in Koordinierung und Steuerung beim CIO verortet werden.

Um hier das „große Ganze“ im Blick zu haben, ist es wichtig, die oben genannte Handlungsfähigkeit in planerischen und haushalterischen Belangen beim CIO zu verorten.

5. **Die Bundeswehr muss die Querschnittlichkeit von IT akzeptieren und sich entsprechend ausrichten.**

Es gibt auch andere Thematiken bzw. Branchen, die eine querschnittliche Bedeutung für die Bundeswehr haben (siehe die Projektelemente wie z.B. Logistik). Aber nur die IT hat eine nahezu vollständige Durchdringungstiefe und Nachhaltigkeit, gemäß dem Motto „IT ist nicht alles, aber ohne IT ist alles nichts.“
IT ist insofern einzigartig, weil

- IT direkt und indirekt angreifbar ist und regelmäßig angegriffen wird
- IT in unterschiedlichen Ebenen implementiert ist (z.B. als administrative Anwendung oder embedded)
- Vernetzung und Schnittstellen vielfältig und komplex sind
- IT sich in sehr kurzen Zyklen weiter entwickelt.
- IT im Gegensatz zur klassischen Rüstung weitgehend „unfassbar“ ist.
- IT auf dem ‚zivilen‘ Sektor vielfältig eingesetzt wird und mit teilweise geringen Adaptionen an die militärischen Anforderungen angepasst werden kann

Die Auswirkungen einer fehlerhaften oder zu engen Umsetzung können finanziell und funktional dramatisch sein.

Es gibt viele Lösungen, z.B. im Big Data Bereich, die querschnittlich eingesetzt werden und damit in völlig unterschiedlichen Nutzungsszenarien zum Einsatz kommen könnten. Da diese Lösungen derzeit nicht querschnittlich, sondern im Rahmen eines Projekts (zum Beispiel für predictive maintainance im Rahmen Projekt A400M) beschafft werden müssten, wird es für dieses eine Projekt zu teuer oder auch zu risikoreich und es bleibt bei ineffizienten Insellösungen.

Beispiele für Querschnittlichkeit:

- Technische Dokumentation
- PKI, Identity- and Access-Management

Um hier besser und vor allem schneller reagieren zu können, müsste der CPM (nov.) um schnellere Verfahren in der IT-Beschaffung ergänzt oder verändert werden.

6. **Der CIO des Verteidigungsressorts muss neben der Rolle des Anforderungsenablers auch in die Umsetzungsverantwortung.**

Bereits in der Stellungnahme zur „IT-Strategie im Geschäftsbereich BMVg“ hat Bitkom angeregt bzw. befürwortet, den IT Direktor (CIO) mit planerischen Freiheiten auszustatten, um die Beschaffung an Architekturprojekten auszurichten. Um die in der Vergangenheit (z.B. beim Ansatz der Vorgabe der TABw) beobachteten „Ausweichstrategien“ einzudämmen und das klare Denken in Richtung Anforderungen, Informationsaustauschbeziehungen usw. mit Blick auf „das was machbar ist“ zu stärken, ist mit Hilfe der Methode Architektur

- ein Gesamtbebauungsplan (Waffensysteme, IT, Personal ...) für die Bundeswehr zu erstellen,
- durch den CIO die Gesamt-IT-Architektur der Bundeswehr (konkret IT-Architekt Bw / CIRK) zu modellieren,
- durch den „Bw-Rüstungs-Architekten“ analog dies für die Rüstung insgesamt zu verantworten,

- die Einhaltung der Architektur-Vorgaben bei allen Rüstungs- und IT-Vorhaben durchzusetzen, zu begleiten und zu kontrollieren,
- Einheitliche Produkte für die gleichen Aufgaben/Fähigkeiten in unterschiedlichen Plattformen und Systemen einzusetzen.

Die im Rahmen der Definition des IPP angelegte Grundidee zu o.g. Forderungen ist personell stärker zu hinterlegen und um den IT-Architekturansatz zu erweitern.

Dazu könnten die im Planungsamt (Abt. IV) erarbeiteten Konzepte, durch gesteuerte Teams den Nutzerbereichen bei der Umsetzung der entsprechenden Vorgaben zu helfen und somit auch die Umsetzung zu kontrollieren, genutzt werden. Zur Vereinheitlichung der IT muss eine entsprechende Stelle geschaffen werden, die diese Vorgaben erstellt, deren Umsetzung begleitet und überwacht (Zentralisierung der Anwendung der Methode Architektur).
Die querschnittlichen Funktionen wie u.a. der Anforderungsmanager („Chefarchitekt der Bundeswehr"), des CIO und des Portfoliomanagers sollten, um die Handlungsfähigkeit sicherzustellen, direkt an die Leitung des BMVg (z.B. in Form eines Stabes) gebunden werden. Nur so kann ohne zusätzliche Steuerungsmechanismen verhindert werden, dass sich die unterschiedlichen beteiligten Abteilungen neutralisieren bzw. gegenseitig lähmen.
Wichtig ist, dass Supply und Demand nicht ohne weiteres zu trennen sind.

7. IT in Waffensystemen muss als Teil einer Gesamtarchitektur verstanden werden.

Eine konsequentere Standardisierung und ein konsequenteres Denken in Lösungen mit Hilfe der Methode Architektur und Schaffung von „Services" über Architekturprojekte würde zwangsläufig eine stärkere Verzahnung zwischen IT und Waffensystemen zur Folge haben, auch könnte so von vornherein das Thema IT-Sicherheit mitbedacht werden. Hierbei ist es von grundlegender Bedeutung, vor dem Denken über Schnittstellen die Anforderungen einschließlich der Cyber-Bedrohungen zu klären. Ohne die Definition von Informationsaustauschbeziehungen („was mit wem") ist die Definition von IT in Waffensystemen nicht Zielführend. Der Anspruch der ITK Branche ist es nicht, Waffensysteme zu bestimmen, aber es sollte der Anspruch aller Beteiligten sein, die Chancen der Digitalisierung zu nutzen. Diese Chancen werden durch voneinander unabhängige und uneffektive Insellösungen nicht genutzt.

Bisher ist es so, dass IT selten (als Ausnahme: SASPF) querschnittlich gedacht wird und deren Beschaffung fast ausschließlich an klassische Rüstungsvorhaben gekoppelt ist.
Die Bundeswehr benötigt einen „Bebauungsplan" (mit einem „Chefarchitekten"), der alle neuen Vorhaben ganzheitlich betrachtet. Aus dieser Sichtweise müssen „querschnittliche Produkte" (also nicht nur IT-Bausteine) definiert und als Vorgabe für die Auswahlentscheidungen herangezogen werden.
IT-Architekturprojekte müssen „Services" als Ergebnis haben, die in einem „Serviceportfolio" (Portfoliomanagement ist zwingend notwendig) zentral bereitgestellt werden. Dabei können durchaus waffenspezifische IT-Komponenten (z.B. der Feuerleitrechner eines Panzers) als „Black-Box" weiterhin sinnvoll sein. Hier muss allerdings übergeordnet die Interoperabilität durch Vorgabe produktunabhängiger Schnittstellen sicher gestellt sein.
Dieses Vorgehen muss auch gegenüber den Auftragnehmern größerer Rüstungsvorhaben (Luft, See, Kampf) durchgesetzt werden, die sich einer kommerziell verfügbaren und einheitlichen IT teilweise immer noch mit dem Hinweis der Risiken bei der Systemintegration verwehren.

8. Eine erfolgreiche Stärkung der IT ist untrennbar mit der Gewinnung und Bindung von Fachpersonal verbunden.

Die Gewinnung und auch die Bindung von IT-Fachpersonal über den Verpflichtungszeitraum hinaus verlangt nach eigenen Laufbahn- und Besoldungsmodellen für den ITK-Bereich. Das hier benötigte Fachpersonal ist eine stark umkämpfte Ressource auch in direkter Konkurrenz mit der gewerblichen Wirtschaft. Deshalb sollten auch in der Vergangenheit verworfene und neue Modelle, welche den Austausch von Personal und Bereitstellung von Reservisten einschließt, konzipiert und umgesetzt werden. Zur Qualifizierung dieses Personals bieten sich ebenfalls Ausbildungskooperationen mit Hochschulen und Unternehmen und dedizierte Reservemodelle für IT-Spezialisten an. Gleichzeitig sollte die Bundeswehr ihren großen Personalpool nutzen, um mit geeigneten Mitteln internes Potenzial zu identifizieren, zu qualifizieren und zu halten. Dies ist nur möglich mit laufbahnbegleitenden Evaluierungselementen und die Eröffnung von Verwendungsvorteilen für das IT-Fachpersonal. Die Schaffung einer „IT-Laufbahn“ sollte angegangen werden. Um die Zeit zu überbrücken, bis die ausgebildeten Fachkräfte zur Verfügung stehen, können auch weitere Kooperationsmodelle entwickelt werden, die über Auslagerung und externe Vergabe bestimmte Dienstleistungen zur Verfügung stellen können.

9. Die IT der Bundeswehr kann einen essentiellen Beitrag zur IT Konsolidierung im Bund leisten.

Zurzeit weisen anderen Bundesressorts in Deutschland in der Informationsverarbeitung noch vergleichsweise hohe Parallelität und Redundanz von Anwendungen und IT-Infrastrukturkomponenten auf. Fertigungstiefe und –umfang bei der Adaption bzw. Integration von handelsüblichen IT-Komponenten sind unterschiedlich ausgeprägt. Die Standardisierung und Konsolidierung in einem ressortübergreifenden Ansatz ist ein aufwendiger und komplexer Prozess, der hinreichend geplant, abgestimmt und sorgfältig durchgeführt werden muss. Hier kann die Bundeswehr Erfahrungen und deren Industriepartner wertvolle Erfahrungen im Sinne Absicherung, Evaluierung und sichere Betriebsführung einbringen.

Eine Standardisierung und Konsolidierung in einem behördenübergreifendem Ansatz hat das Potenzial für erhebliche Verbesserungen und Einsparungen. Als erster Schritt sollte die konsequente Zentralisierung der heute noch verteilt organisierten IT-Unterstützung für die Ämter und Dienststellen der verschiedenen Ressorts sowie eine stringente Anwendungskonsolidierung weiter vorangetrieben werden, da hier die größten Ersparnisse zu vermuten sind. Auch die Bundeswehr kann dies nutzen, um heute noch für behördliche Standardaufgaben gebundene Kapazitäten für verteidigungs- und sicherheitsrelevante Aufgaben einsetzen zu können. Gerade im Hinblick auf die asymmetrische Bedrohungslage aus und im Cyber-Raum sollte neben der Zentralisierung als Bestandteil einer umfassenden Konsolidierung auch eine bewusste Schaffung bzw. Erhaltung von Resilienz erwogen werden.

Mit dem Beschluss des Haushaltsausschuss von Mai 2015 wurde die Konsolidierung beschlossen. Mit ihrer bereits heute leistungsfähigen IT eignet sich die Bundeswehr als Dienstleister für andere Ressorts. Mit den am 17.09.2015 angekündigten Veränderungen kann es gelingen, die IT und die Cyber-Fähigkeiten der Bundeswehr auf eine neue Stufe zu heben. Damit ist diese IT/Cyber-Organisation prädestiniert für Anforderungen der äußeren Sicherheit zu etablierende Technologiekomponenten und Verfahren im Rahmen der ressortübergreifenden Anstrengungen einzubringen und somit einen nachhaltigen Beitrag zu leisten um die Cybersicherheit in Deutschland deutlich zu erhöhen.