Verteidigung

Die Bundeswehr ins Zeitalter der Digitalisierung führen

Bitkom-Positionen für ein digitales Deutschland

Mit der Neuordnung des Cyber- und Informationsraums gehen das Bundesverteidigungsministerium (BMVg) und Bundeswehr konsequent einen neuen Weg. In den vergangenen Jahren wurde mit Fähigkeiten zur vernetzten Operationsführung, Einführung bundeswehrweiter Unternehmenssoftware, ersten Reaktionsfähigkeiten im Bereich Cyberabwehr, sowie der Privatisierung administrativer Informationstechnik, die Digitalisierung in der Bundeswehr vorangetrieben. Mit einem neuen militärischen Organisationsbereich werden erstmals in der Bundeswehr IT und Cyber als Fähigkeiten betrachtet, die auch intern endlich die Gewichtung erhalten, die der realen (Bedrohungs-)Lage angepasst sind. Der gewählte Ansatz ist auch international richtungweisend. So konsequent haben bisher nur wenige Nationen die Bedeutung von IT und Cyber auf der organisatorischen Seite abgebildet.

1. Status Quo

- Im Rahmen des Weißbuch-Prozesses reagierte die Bundesregierung auf die sich ständig verändernden sicherheitspolitischen Rahmenbedingungen. Dabei stehen auch Phänomene wie hybride Kriegsführung und Cyber Defense im Fokus. Weitere Programme wie die Agenda Rüstung, Agenda Attraktivität, Trendwende Personal und Trendwende Finanzen sollen dafür sorgen, dass die Bundeswehr den Anforderungen der Einsatzwirklichkeit im 21. Jahrhundert demographiefest gerecht wird.
- Eine fortgeschriebene IT-Strategie, ein CIO auf Abteilungsleiterebene (Abteilung CIT) und ein herausgehobener militärischer Organisationsbereich (CIR) unterstreichen auf organisatorischer Ebene die Bedeutung einer teilstreitkräfteübergreifenden Vorgehensweise. Diese Konsequenz in der Konzeption sucht auch international seinesgleichen und erfährt deshalb viel Beachtung.
- IT und Rüstung müssen zusammen gedacht, entwickelt und eingesetzt werden. Allerdings passen die Längen der Innovations- und Beschaffungszyklen nicht zusammen.

2. Ziele

- **Konsequente Umsetzung der Neuorganisation**: Die begonnene Neuorganisation im Bereich Cyber/IT muss fortgesetzt werden, denn nur so kann die Bundeswehr ihren Aufgaben auch in Zukunft gerecht werden. Das gilt vor allem für die Abteilung CIT und das Kommando CIR, deren Konzeption mit allen dazugehörigen Faktoren nachhaltig umgesetzt werden muss. Dafür muss ein ressortübergreifender Konsens erzielt werden, dass die eingeleiteten Maßnahmen nur greifen können, wenn der dahinterliegende Sinn von allen Beteiligten gelebt wird.
- **Digitalisierung der Bundeswehr umfassend weiterdenken**: Die Bundeswehr muss sich innovativ und ganzheitlich im Bereich IT und Cyber weiterentwickeln. Den Innovationszyklen der IT sollte bedarfsorientiert und zeitnah gefolgt werden. So können auch neue Trends gesetzt werden. Dadurch kann sich die Bundeswehr auf dem Arbeitsmarkt als moderner und attraktiver Arbeitgeber positionieren. Um den Transformationsprozess des BMVg und der Bundeswehr fortzusetzen, sollte sich das Kommando CIR diesen Themen ganzheitlich widmen.

Stand: 24.01.2018

bitkom

- Zeitgemäße Beschaffungsstrategien entwickeln: Die Streitkräfte müssen sich in der Beschaffung neuer IT-Lösungen von dem Ansatz teurer Eigenproduktionen und Insellösungen verabschieden. Dabei müssen auch die in der IT-Strategie geforderten weltweit eingeführten Standards nutzbar gemacht werden. Darüber hinaus kann die Bundeswehr durch frühzeitiges Aufgreifen neuer Entwicklungen selber Standards setzen.

3. Politische Vorschläge

- **Kritische Überprüfung der Zuständigkeitsverteilung**: Es sollte möglichst schnell geklärt werden, inwieweit die Zuständigkeiten zwischen den Ressorts sinnvoll verteilt sind. Die Verteidigung des Cyber- und Informationsraumes ist eine gesamtstaatliche Aufgabe, deren Ziele, Zuständigkeiten und Befugnisse klar umrissen werden müssen. Nicht zuletzt für die Wirtschaft ist es wichtig, die relevanten Institutionen klar benennen zu können.
- **Bedürfnisse der Soldaten in den Vordergrund stellen**: Die Interessen aller Gruppen innerhalb des Verantwortungsbereiches des Verteidigungsministeriums müssen an den Bedürfnissen der Soldaten im Einsatz (schneller, interoperabler und funktionaler Zulauf von Ausrüstung) ausgerichtet werden.
- **Schnellere IT-Einführung gewährleisten**: Eine schnellere IT-Einführung ist notwendig, um mit den kurzen Innovationszyklen der Digitalwirtschaft Schritt halten zu können und damit Führungsfähigkeit und Informationsüberlegenheit gegenüber einer Bedrohung aus dem Cyber- und Informationsraum sicherzustellen.
- **Guten Austausch zwischen den Akteuren weiter stärken**: Die hohe Dialogbereitschaft des Ministeriums im Rahmen der Neuorganisation muss beibehalten werden und nach dem Modell des Weißbuch-Prozesses fortgeführt und gestärkt werden. Nur durch einen engen und uneingeschränkt offenen Austausch mit der Wirtschaft kann das Ministerium die hoch gesteckten Ziele der Neuorganisation erreichen. Das BMVg sollte sich in diesem Sinne aktiv am Digital-Gipfel-Prozess der Bundesregierung beteiligen.
- **Stärkere Bündelung innovativer Kräfte in Betracht ziehen**: Es sollten grundsätzliche Überlegungen angestellt werden, schrittweise ein mit der Wirtschaft betriebenes »Zentrum für digitale Innovationen« aufzubauen, um einen produktiven Austausch zu institutionalisieren. So könnten die Entwicklung und der Betrieb von z. B. Cyber- und Big Data-Analytics-Szenarien oder mobilen Anwendungen sowie deren Steuerung sowohl für den militärischen wie auch den nicht militärischen Bereich von einem solchen Zentrum übernommen werden.
- **Attraktive Arbeitsbedingungen schaffen im Kampf um Fachkräfte**: Im Kampf um die klugen Köpfe müssen moderne und attraktive Arbeitsbedingungen geschaffen werden, die mit der freien Wirtschaft konkurrieren können.
- **Finanzielle Ressourcen richtig investieren**: Die bis 2020 um mehr als 10 Milliarden Euro aufgestockten Finanzmittel des EPl 14 müssen effektiv für Cyber und IT genutzt werden. Daher sollten große Teile dieses Geldes für den Aufbau der Cyber-Fähigkeiten und der Organisationsbereiche der Abteilung CIT und des Kommandos CIR sowie für das notwendige IT-Personal und Projekte genutzt werden.

Ihr Ansprechpartner

Teresa Ritter | Referentin Sicherheitspolitik
T 030 27576-203 | t.ritter@bitkom.org

Albrechtstraße 10 | 10117 Berlin
www.bitkom.org

bitkom