Auswertung des Abschlussberichts des Aufbaustab Cyber- und Informationsraum

Update 06, 25.03.2017

Thomas Reinhold, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, reinhold@ifsh.de, http://cyber-peace.org

Mit der Veröffentlichung des Abschlussbericht Aufbaustab Cyber- und Informationsraum stehen der Bundeswehr und dem BMVg vor allem einige Veränderungen ins Haus. An dieser Stelle sollen die wichtigsten Änderungen zusammengefasst werden, dabei neben den strukturellen Änderungen (die im Abschlussbericht in aller gebotenen Detailtiefe nachzulesen sind) vor allem die Implikationen hinsichtlich des Ausbaus offensiver Fähigkeiten der Bundeswehr im Cyberspace und den damit verbundenen friedens- und sicherheitspolitischen Aspekte eingehen.

Zum 1. Oktober 2016 wird im Bundesverteidigungsministerium eine Abteilung Cyber/ IT (CIT) eingerichtet und (vermutlich) mit dem ThyssenKrupp-Manager Klaus-Hardy Mühleck in der Rolle eines Chief Information Officer (CIO) besetzt. Auf militärischer Seite wird zum 1. April 2017 mit der Aufstellung eines neuen Organisationsbereichs für den Cyber- und Informationsraum begonnen (KdoCIR) und durch eine/n Inspekteur/in geleitet. **[Update 29.4.2016]** Dem Tagesbefehl der Verteidigungsministerin vom 26.4.2016 zufolge wird diese Funktion Generalmajor Ludwig Leinhos übernehmen. **[Update 22.6.2016]** Die beiden Posten sind dabei Aussagen der Verteidigungs-minsterin zufolge auch explizit als zentrale Ansprechpartner für internationale Kontakte und Bündnispartner gedacht. Diese sogenannten “points of contact” sollen dabei ein bessere Harmonisierung und Abstimmung im Rahmen von Allianzen ermöglichen. Damit werden vermutlich unter anderem die NATO-Pläne addressiert, Angriffe im Cyberspace in den Kanon Beistandspflichten nach Artikel-5 des NATO-Vertrages aufzunehmen[1]. Die Umstrukturierungs- und Aufbauarbeiten sollen bis 2021 abgeschlossen sein und bis zu 20.000 Personen und Dienststellen betreffen. Die im Abschlussbericht genannten Personalstärken verdeutlichen, dass dies insbesondere zum Start in erster Linie mit Umstrukturierungen bestehender Kapazitäten erfolgen wird. Für die neue Abteilung CIT beim Bundesverteidigungsministerium wird ein "anfänglicher Bedarf von ca. 130 Dienstposten", gesehen, "von denen voraussichtlich 95 Dienstposten übertragen werden können". Im Bereich der militärischen Strukturen des KdoCIR werden 13.700 Dienstposten zusammengeführt, von denen der überwiegende Teil (12.800 Dienstposten) dem aktuellen Bereich der Streitkräftebasis (SKB) entstammt. Die Auflistung der Wanderungsbewegung zeigt, dass ohnehin bereits ein Gutteil der IT-relevanten Aufgaben und Fähigkeiten in Bereich der Streitkräftebasis zusammengeführt sind: Führungsunterstützungskommando (FüUstgKdoBw), Kommando Strategische Aufklärung (KdoStratAufkl), Zentrum für Operative Kommunikation der Bundeswehr

[1] http://cyber-peace.org/2016/06/15/nato-cyber-offiziell-auch-bestandteil-der-buendnis-verteidigung/

(ZOpKomBw) und Teile des (zivilen) Bundesamts für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr mit dem angeschlossenen IT-ZentrumBw. **[Update 11.5.2016]** Der Tagesbefehl zur allgemeinen Veränderung der Personalstruktur der Bundeswehr vom 10.5.2016[2] zufolge sollen im Zuge des OrgBereichs CIR sowie den dargestellten Umstrukturierungen im BMVg 1648 neue militärische Dienstposten und 316 neue zivile Dienstposten bis 2021 entstehen. Die Zahlen gehen aus einer Analyse-Grafik des deutschen Bundesverbands (Abb. 1 im Anhang) hervor.

Änderungen beim BMVg, der Bereich Cyber/IT

Im Bereich des Änderung des BMVg erstrecken sich die Änderungen dabei vor allem auf die Umsetzung von Kernzielen wie der Effektivierung von IT Projekten, deren Planung, Beantragung, Budgetierung sowie dem agilen (anforderungsbezogenen) Management bei Beschaffung, Entwicklung und Forschung. "Die ministerielle Steuerung sowohl der technologischen/ technischen Weiterentwicklung von Cyber/ IT als auch von Einsatz, Betrieb und Schutz der IT des Verteidigungsressorts erfolgt [damit] aus einer Hand". Die Besetzung der Leitung mit einem Manager aus der freien Wirtschaft soll es dem BMVg ermöglichen bei der technischen Ausrüstung auf dem Stand der aktuellen IT zu gelangen und langfristig mit diesem Schritt zu halten. Konzeptionell wird die Abteilung CIT in zwei Unterabteilungen gegliedert:

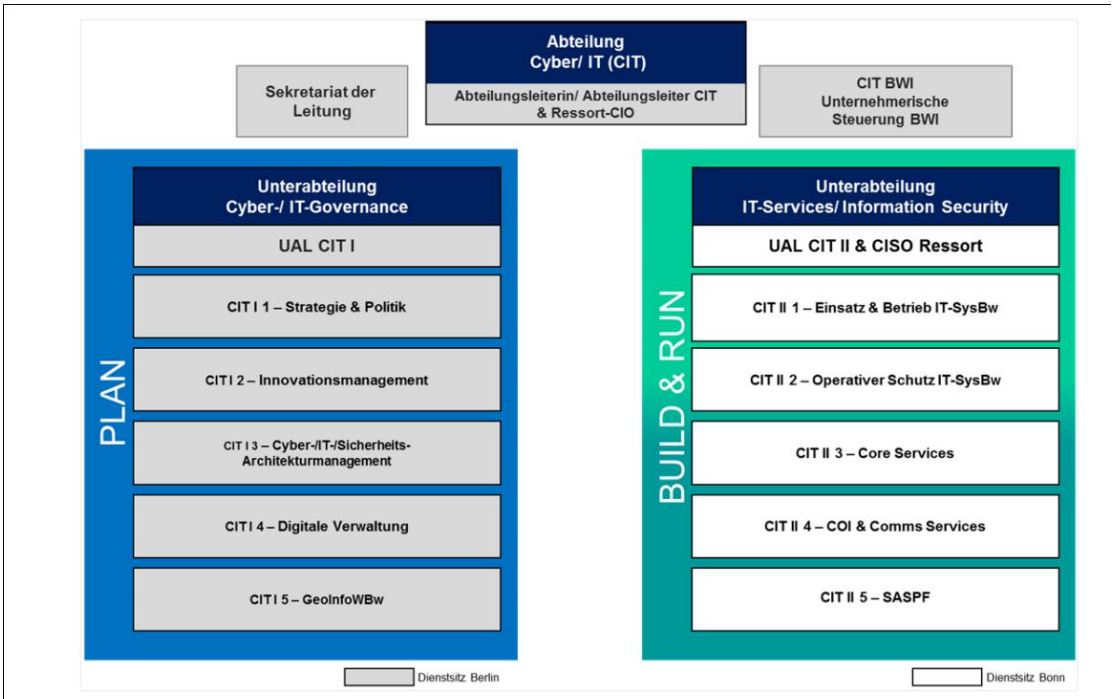


Abbildung 4: Abteilung Cyber/ IT im BMVg

2 http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYvBCsIwEET_aDcBRfTWUA9eRdB6S9sQVppNWTf14sebHJyBd5jH4BNr2W8UvVJmv-ADh4lO4wfGtEV45SJ1hURMbw1CJeG9feYAU-agjRpYqTKK1yywZtGlmSJSDdCMg7G9M9b8Y7_d8XbeObs_9Bd3xTWl7gdG82aA/

Eine genaue Beschreibung der einzelnen Bereiche und ihrer zugedachten Aufgaben ist im Abschlussbericht ab Seite 20ff zu finden und es soll an dieser Stelle auf eine Kopie verzichtet werden.

Änderungen im Bereich der Bundeswehr: das Kommando Cyber- und Informationsraum (KdoCIR)

Im Bereich der Bundeswehr umfassen die strukturellen Maßnahmen in erster Linie die Zusammenführung und den Ausbau von Kapazitäten im Bereich der operativen Maßnahmen im Cyberraum (beginnend mit dem elektronischen Kampf, dem militärischen Nachrichtenwesen, den Aufgabenbereichen der Aufklärung, operativer Kommunikation und Lagebilderstellung sowie den Kräften der offensiven Computer Network Operations) und der Kapazitäten im Bereich der IT-Sicherheit, Sicherung und technischer Weiterentwicklung. Darüber hinaus soll die Weiterentwicklung und Ausbildung (berufsqualifizierende Aus-, Fort- und Weiterbildung) des gesamten Kommandobereichs CIR direkt Aufgabe des Inspekteurs und den Abteilung des Führungsstabs werden und dieser damit ein "richtungsgebenden Funktion" zukommen.

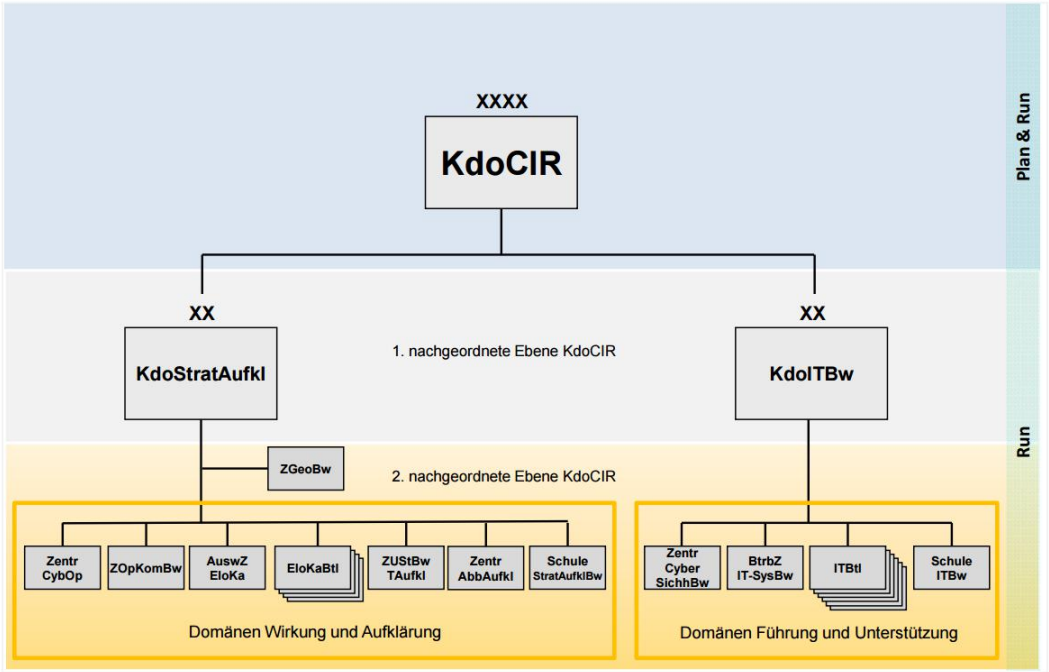


Abbildung 5: Startaufstellung Organisationsbereich Cyber- und Informationsraum 2017

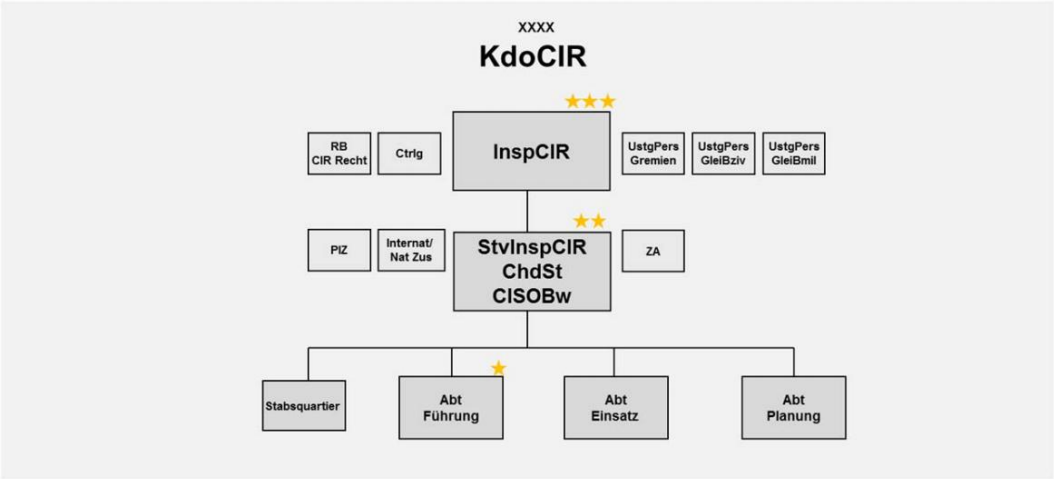


Abbildung 6: Startaufstellung KdoCIR 2017

Eine detaillierte Beschreibung der einzelnen Abteilungen ist im Abschlussbericht ab Seite 22ff zu finden, ein Abkürzungsverzeichnis ab Seite 40.

Wichtige Implikationen sowie friedens- und sicherheitspolitische Aspekte

Unabhängig von den strukturellen Änderungen sollen nachfolgend eine Aspekte des Abschlussberichtes hervorgehoben werden, die insbesondere mit Blick auf den Ausbau der offensiven Fähigkeiten der Bundeswehr im Cyberspace, die damit verbundenen friedens- und sicherheitspolitische Aspekte sowie auf eine mögliche außenpolitische Wirkung eingehen. Eine genauere Analyse der einzelnen Punkte kann nur in den kommenden Wochen und Monate schrittweise erfolgen.

- Der Bericht betont die Auffassung des Cyberspace und der Bedrohungen als eine "gesamtstaatliche" Aufgabe im Bund, die im Sinne einer Umsetzung der Strategischen Leitlinie Cyber-Verteidigung von 2015 in ressortübergreifender Kooperation mit den Bundesinnenministeriums realisiert werden soll. Dabei wird explizit auch der Schutz kritischer Infrastrukturen genannt.

  > *In Bezug auf die Frage der Zusammenarbeit in der Cyber-Sicherheit und -Verteidigung, der fließenden Grenzen zwischen innen und außen, haben deshalb BMI und BMVg ein gemeinsames Verständnis der komplementären und eng verzahnten Aufstellung entwickelt: - Die Wahrung der Cyber-Sicherheit ist eine gesamtstaatliche Aufgabe, die nur gemeinsam zu bewältigen ist. - Dazu gehört auch der gemeinsame Schutz der Kritischen Infrastrukturen.*

  In Bezug auf den Schutz von Kritischen Infrastrukturen stellt sich zum einen die Frage, aus welchem Grund dieser nicht originäre Aufgabe des BSI, als zivile und bereits mit dieser Aufgabe betraute Institution bleibt. Welche unterstützende

Leistung soll die Bundeswehr hier erbringen und kann sie die dafür notwendigen Ressourcen und das Know-How verfügbar machen, trainieren und dieses für einen Einsatzfall verfügbar halten, ohne dass Doppel-Verantwortlichkeiten zu anderen Diensten entstehen. Unklar ist auch, wie ein solch kontinuierlicher Schutz und eine beständige Abwehr von IT-Gefährdungen mit den sehr engen Grenzen eines Bundeswehr-Einsatzes im Inneren harmonieren kann und wie die praktikable Zusammenarbeit der Dienste ohne Vermengung innen- und außenpolitischer Belange umgesetzt werden soll. Unter der Annahme dass die Bundeswehr einen Schutz zwar in enger Abstimmung, jedoch nur außerhalb Deutschlands leisten soll, ist zu hinterfragen, in welchem Rahmen damit "active defense"-Maßnahmen ergriffen werden müssen, die Eingriffe in fremde Netze (die ggf. nicht unter Hoheit des Angreifers sondern unbeteiligter Dritter stehen) erfordern. Derartige Maßnahmen ("Hack-Back", "Vorneverteidigung", "active defence") werden lt. Aussage von Stsin Dr. Suder in der Anhörung im Verteidigungsausschuß vom 22.2.2016 zwar geprüft, sind aber gegenwärtig nicht geplant[3].

- Hinsichtlich der Kooperationen der Bundeswehr mit anderen nationalen Institutionen könnte eine engere Vernetzung der Dienste eine immer stärkere Vermischung der Grenzen zwischen den Aufbau defensiver Fähigkeiten und dem Aneignen von Wissen zu offensiven Operationen und entsprechender Angriffsvektoren führen das über die dafür speziell vorgesehene Einheit der Computer Network Operations hinaus geht:

  > *"Der CIR kennt weder nationale Grenzen noch ein hierarchisches oder institutionelles Gefüge. Selbst die Grenze zwischen offensiver und defensiver Ausrichtung ist fließender als sonst. Hat ein Akteur die Fähigkeit zur Verteidigung, so kann er auch weltweit angreifen. - Hierdurch verschwimmen die Grenzen zwischen Krieg und Frieden, innerer und äußerer Sicherheit sowie kriminell und politisch motivierten Angriffen."*

  Eine solche Vermischung würde in erster Linie weitere innenpolitische Fragen der Trennung von Diensten mit Blick auf deren Befugnisse, Grenzen und parlamentarischen Kontrollmöglichkeiten hervorrufen.

- Im Bereich der Kooperation mit nationalen Nachrichtendiensten stellt der Bericht eindeutig fest, dass

  > *"Das System Militärisches Nachrichtenwesen mit seinen gesetzlichen Regelungen und das Verhältnis Militärisches Nachrichtenwesen, Bundesnachrichtendienst und Militärischer Abschirmdienst stehen nicht zur Disposition."*

---

[3] http://www.bundestag.de/bundestag/ausschuesse18/a12/oeffentliche_anhoerung/cyber1/405094

Eine solche Zusammenarbeit wäre bspw. mit Blick auf die notwendige Aufklärung und Informationsgewinnung in Friedenszeiten für umfassende Lagebilder im Sinne der Strategischen Leitlinie Cyber-Verteidigung und der Identifikation von Angriffsvektoren und Schwachstellen bei potentiellen militärischen Zielen notwendig.

- Im Bereich der Fachkräftegewinnung wird die Bundeswehrhochschule in München zu der zentralen, wissenschaftlichen Aus-, Fort und Weiterbildungsstätte (..) für Tätigkeiten im Bereich der Cyber-Verteidigung und Cyber-Sicherheit ausgebaut. **[Update 22.6.2016]** Dort soll ein Studiengang "Cyber-Sicherheit" aufgebaut werden, der ab 2018 beginnen und bis zu 70 AbsolventInnen pro Jahr ausbilden soll:

  > *Auch die bereits an der Universität der Bundeswehr München bestehenden Möglichkeiten einer wissenschaftlichen Aus-, Fort- und Weiterbildung in einschlägigen Studienfächern des MINT-Spektrums sind zu stärken und auf die Handlungsfelder im Bereich MilNW und Cyber-Verteidigung auszurichten*

  [Update 25.03.2017] Im Rahmen des 2013 gegründeten Forschungszentrum Cyber Defence (CODE) 2013 werden durch das BMVg 11 neue W3-Professuren mit 67 Mitarbeitern finanziert. Weitere 200 Mitarbeiter sind durch Drittmittelfinanzierungen zugesagt. Außerdem entsteht für einen zweistelligen Millionbetrag ein 7000 Quadratmeter große Gebäude mit 8 Hightech-Labs für die Cyber-Forschung (Quelle: https://heise.de/-3287684).
  Eine entsprechende Intensivierung wird sich jedoch vermutlich frühestens am Ende des anvisierte Planungsrahmen 2021 auswirken. Damit bleibt offen, wie die notwendigen Fachkräfte für die nächsten Jahre geworben werden sollen - insbesondere im Bereich der IT und den zumeist attraktiveren Gehalts- und Karriereaussichten in der freien Wirtschaft. Ferner wird bei der Ausgestaltung des Curriculum des Studiengangs eine wichtige Betonung der "Ausbildung zur Verteidigung" nötig sein. Aus technischer Sicht ist eine klare Trennung nur schwer möglich und ein Erlernen von Abwehr-Möglichkeiten schließt zumeist den Erwerb offensiver Fähigkeiten mit ein. Angesichts der bisher unklaren Regelungen zu offensiven Fähigkeiten, deren strategischen Einsatz sowie den Grenzen und der notwendigen parlamentarische Kontrolle ist hier eine deutliche Eingrenzung auf defensive Fähigkeiten notwendig.

- **[Update: 29.4.2016]** Der Abschlussbericht erkennt an, dass ausgebildete IT-Fachkräfte auf dem freien Markt deutlich attraktivere Konditionen für eine Beschäftigung hinsichtlich Vergütung und Karriere vorfinden. Einem BITKOM-Bericht von Ende 2015 zufolge fehlen selbst in den

ITK-Unternehmen in 6 von 10 Fällen Fachkräfte[4]; insgesamt gibt es rund 43.000 offene Stellen. Dieser Mangel hat sich gegenüber den Vorjahren verschärft. Der Bericht schlägt daher neben der verstärkten Zielgruppen-Werbung die Einrichtung von Speziallaufbahnen vor, die diesen Wettbewerbsbedingungen gewachsen sind. Dabei werden unter anderem auch eng verzahnte Wirtschaftskooperationen angestrebt, um Fachkräfte aus der Wirtschaft für Bundeswehr-Einrichten zu gewinnen, diese ggf. später wieder in die Wirtschaft abzugeben und im Stile von Reservisten vorzuhalten. Vor diesem Hintergrund wird die Entwicklung bei Gesprächen mit Partnern aus der Wirtschaft, Verhandlungen zu Public-Private-Partnership-Abkommen etc. Aufschluss über den Umfang von dermaßen gewonnen Fachpersonal und dem damit verbundenen Know-How liefern. Da IT-Security sowohl im defensiven, als auch im offensiven Bereich in erster Linie dem Know-How von Personal entspringt und erst nachrangig eine Frage der richtigen Technik ist, könnten entsprechende Kooperation auch als eine alternative “Quelle” zu klassischen Rüstungsprojekten und langjährigen Beschaffungsverfahren darstellen.

- In Ergänzung eines Strategiepapiers des Bundeswirtschaftsministerium von 2015 wird nun neben Fähigkeiten der Kryptographie auch explizit die Fähigkeiten in "allen vier Fähigkeitsdomänen der Bundeswehr (..) Führung, Aufklärung, Wirkung und Unterstützung" leisten zu können als nationale Schlüsseltechnologien benannt und entsprechend deren Entwicklung in Deutschland als "eine wesentliche Säule für die Zukunftsfähigkeit der Bundeswehr im Cyber- und Informationsraum" und folglich zu stärkender oder aufzubauender Industriebereich betrachtet. Eine Aussage des Beauftragten für die strategische Steuerung nationaler und internationaler Rüstungsaktivitäten der Bundeswehr Gundbert Scherf zufolge werden bereits 10% der F&T-Mittel (Forschung und Technologie) in die Entwicklung von IT investiert. Dieser Umfang soll nochmals überdacht werden.

- Das Wirken und die Verteidigung im Cyberspace wird im Abschlussbericht als ein entscheidender militärischer Entwicklungssprung angesehen und in einer Grafik als nächster Schritt nach der Entwicklung des Panzers und der Nuklearwaffen illustriert. Folglich betont der Abschlussbericht die Bedeutung die einer Verteidigung aber auch der offensiven Wirkung in diesem Bereich zukommt, insbesondere angesichts der betonten Entwicklung anderer Nation in diesem militärischen Sektor. Dabei wird auch das "Wirken im Cyber- und Informationsraum auch als eigenständige Operation" als Option erwogen.

  > *Operationen, die nur im CIR stattfinden, sind denkbar, jedoch sind die über den CIR erzielbaren Effekte grundsätzlich Teil einer Streitkräfte-gemeinsamen Operation.*

[4] https://www.bitkom.org/Presse/Presseinformation/43000-offene-Stellen-fuer-IT-Spezialisten.html

- Die Notwendigkeit der Fähigkeit zur offensiven Cyberwirkung und deren aktuelle Form der Einheit "Computer Network Operations" (CNO) wird deutlich betont und ausgebaut und soll bereits zum Beginn des KdoCIR im April 2017 um 20 Dienstposten aufgestockt werden, gegenüber dem aktuellen offiziellen Personalumfang von 60 Dienstposten. Die Einheit wird in Form eines eigenen Zentrums für Cyberoperationen zentral aufgestellt soll zukünftig auch personell weiter aufgestockt werden.

  > *In der Startaufstellung 2017 wird die Gruppe für Computer Netzwerk Operationen (CNO) zur Stärkung von Aufklärung und Wirkung im Rahmen der Cyber-Verteidigung zu einem eigenständigen Zentrum Cyber-Operationen ausgebaut und dem KdoStratAufkl direkt unterstellt. (..) Ziel der weiteren Entwicklung ab 2018 sind [u.a.] die Stärkung der Fähigkeiten im Bereich Cyber-Lage, die an die Erfordernisse von Einsätzen angepasste schicht- und durchhaltefähige Ausgestaltung der Fähigkeiten zur Aufklärung und Wirkung im Cyber-Raum. (..) Für diesen weiteren Ausbau vorhandener sowie den Aufbau zusätzlich erforderlicher, zeitgemäßer Fähigkeiten zur Durchführung von Cyber-Operationen werden zusätzliche Dienstposten benötigt.*

- Die Entwicklung aktiver Wirkungsmittel im Cyberspace wird flankiert von einer engen Anbindung der Einheiten des militärischen Nachrichtenwesens (MilNW) und der militärischen Aufklärung im KdoCIR. Ziel und eine zentrale Aufgabe des gesamten Organisationsbereiches ist das

  > *Erstellen einer umfassenden militärischen Nachrichtenlage sowie eines übergreifenden Cyber Lagebildes und Beitragen zu einem gesamtstaatlichen Lagebild*

  *W*ie bereits erwähnt kann auch diese enge Verzahnung und organisatorische Verbindung als eine mögliche Maßnahme gewertet werden um Informationen über relevante militärische Ziel zusammen zu tragen und für Aufgaben der CNO-Einheiten vorzuhalten. Eine entsprechende Betonung der damit verbundenen notwendigen Präsenz der Dienste in fremden Netzen kann von anderen Nationen aber als ein starkes Signal verstanden werden, ihrerseits defensive und offensive Maßnahmen auszubauen.

- Im Rahmen des Ausbaus der Cyber-Fähigkeiten soll auch insbesondere auf die Anforderungen im Rahmen von Kooperationen mit anderen Nationen eingegangen und den Verpflichtungen aus Bündnissen Rechnungen getragen werden

  > *Der Stab KdoCIR soll zur vollständigen Aufgabenwahrnehmung ausgebaut und in den Fachaufgaben Planung und Recht gestärkt werden. Der Aufbau der*

Fähigkeiten zur Planung und Führung von Operationen sowie die Fähigkeit einen substanziellen Beitrag zu einem multinationalen CommandElement zu leisten, wird durch den Aufwuchs der Abteilung Einsatz im Stab KdoCIR erreicht, insbesondere in Anbetracht der internationalen Entwicklungen bei Partnern („Cyber-Kommandos“) und in der NATO („Cyber as a Domain“) (..) [ist] das Vorhalten eines multinationalen Kommandoelements für den CIR erforderlich

Ergänzende Anmerkungen zu den Zielen der Umbau-Maßnahmen [Update 24.5.20160]

In einem, auf den Seiten des BMVg am 5.4.2016 veröffentlichten Artikel[5] von James A. Lewis vom US Center for Strategic and International Studies geht dieser auf die Herausforderungen und gestiegenen Anforderungen durch Cyber als potentielle militärische Domäne ein. Dieser Beitrag "Der Cyberspace und die Streitkräfte" wurde auf den Webseiten mit dem Vermerk, dass er ausschließlich die Meinung des Autors wiedergibt veröffentlicht. Der Zeitpunkt der Veröffentlichung, die Bezugnahme zu jener Aufgabenstellung, denen sich auch der Aufbaustab gewidmet hat und die Publikation des Beitrags im Rahmen der Diskussion um das Weißbuch 2016 räumen den Aussagen jedoch eine gewisse Relevanz ein. Einige der Gedanken des Beitrags sollen daher an dieser Stelle ergänzend zu den obigen Überlegungen und Analysen zitiert werden. Ein detaillierte Nachlese des Beitrags ist sehr empfehlenswert.

- *Staaten tun dies* [die militärischen Cyber-Fähigkeiten in eine Art von „Cyber-Kommando" zusammenzufassen, einem geschlossenen militärischen Bereich, der die bestehenden Cyber-Elemente zu einer kohärenten Einheit bündelt]*, weil ein Cyber-Kommando viele Vorteile bietet. Zum einen fördert es die Koordination, was wiederum die Verteidigungsmöglichkeiten verbessert und die „Entflechtung" von Angriff und Verteidigung erleichtert. Zum anderen erleichtert es die Beschaffung von Cyber-Mitteln und -Ausbildung und spart Kosten (der Ausbildungsaufwand sollte nicht unterschätzt werden). Die USA stellten als erstes Land ein Cyber Command auf (anfänglich als Defensivmaßnahme, um die Koordinierung unter den defensiv ausgerichteten militärischen Elementen zu verbessern). Die Streitkräfte größerer Länder folgen jetzt ihrem Beispiel.*

- *Militärische Cyber-Fähigkeiten werden auch in den Fokus von Bündnisverpflichtungen rücken. Die NATO ringt mit ähnlichen Fragen in Bezug auf offensive Fähigkeiten, aber angesichts verschärfter Spannungen und neuer Arten von Konflikten (zum Beispiel hybride Kriegsführung) ist es schwer vorstellbar, wie die NATO eine glaubhafte Abschreckung ohne Zugriff auf das gesamte Spektrum an Cyber-Fähigkeiten sicherstellen kann. Niemand wird ernsthaft verlangen, dass die NATO sich mit Flugabwehrsystemen zufrieden geben und auf Jagdflugzeuge verzichten sollte. Mit den Cyber-Fähigkeiten verhält es sich ähnlich. Die Beschaffung von Cyber-Angriffsmitteln durch die NATO (im Sprachgebrauch der NATO „aktive Abwehr") verpflichtet das Bündnis, neue Erfordernisse zu definieren. Die Verantwortlichkeiten für Führung und Genehmigung von Cyber-Angriffen sind explizit festzulegen und in reguläre Planungen, Übungen und Konsultationen aufzunehmen. Gleiches gilt für nationale Cyber-Fähigkeiten.*

---

5 http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYs7DsIwEAVvtGsXSIQuViRECQ0knX8yFvE6cjZJw-GxC95I04weTlghvcegOWbSM75wtPFiDjBpD3D4uK5ms28I3mn6eMJnuzgPNpPnZvbEsToUzbnAkgvPrWyl1ALR4SjkoIQU_8lvf75fJ3XquuGmHrik1P8A3_4wUQ!!/

- *Unsicherheit kennzeichnet die Nutzung militärischer Cyber-Fähigkeiten, wenn man vom heutigen Stand der Technik ausgeht. Nicht immer wissen wir, welche Einrichtungen mit anzugreifenden Netzwerken verbunden sind. Es könnte ein Krankenhaus sein oder eine andere zivile Einrichtung, die kein legitimes Ziel darstellt. Darüber hinaus besteht stets die Sorge, dass der Angriff auf ein legitimes militärisches Ziel außer Kontrolle gerät und unschuldige Zivilisten treffen könnte. (..) Das Risiko von Kollateralschäden lässt sich durch die Schaffung nachhaltiger Führungsstrukturen für Cyber-Operationen und –Mittel vermindern.*

- *Cyber-Aktionen zur Gewinnung von militärisch wertvollen Informationen sind wichtig, stellen aber keinen Angriff dar. Die Fähigkeiten und Mittel sind ähnlich, aber ein klarer Unterschied liegt darin, dass die Nachrichtengewinnung die Entscheidungsfindung unterstützt, während Angriffe diese stören. Cyber-Spionage und Cyber-Angriff überschneiden sich in erster Linie in der Notwendigkeit, sicherzustellen, dass Spionageaktivitäten gegen Netzwerke mit militärischen Cyber-Operationen abgestimmt werden, so dass sich diese nicht gegenseitig stören. In dieser Hinsicht kann ein zentrales Kommando von unschätzbarem Wert sein.*

Anmerkung zu den Quellen und Zitaten: Alle Zitate entstammen, sofern nicht abweichend angegeben dem "Abschlussbericht Aufbaustab Cyber- und Informationsraum des BMVg", April 2016[6] oder den Folien der Präsentation des Berichtes[7]

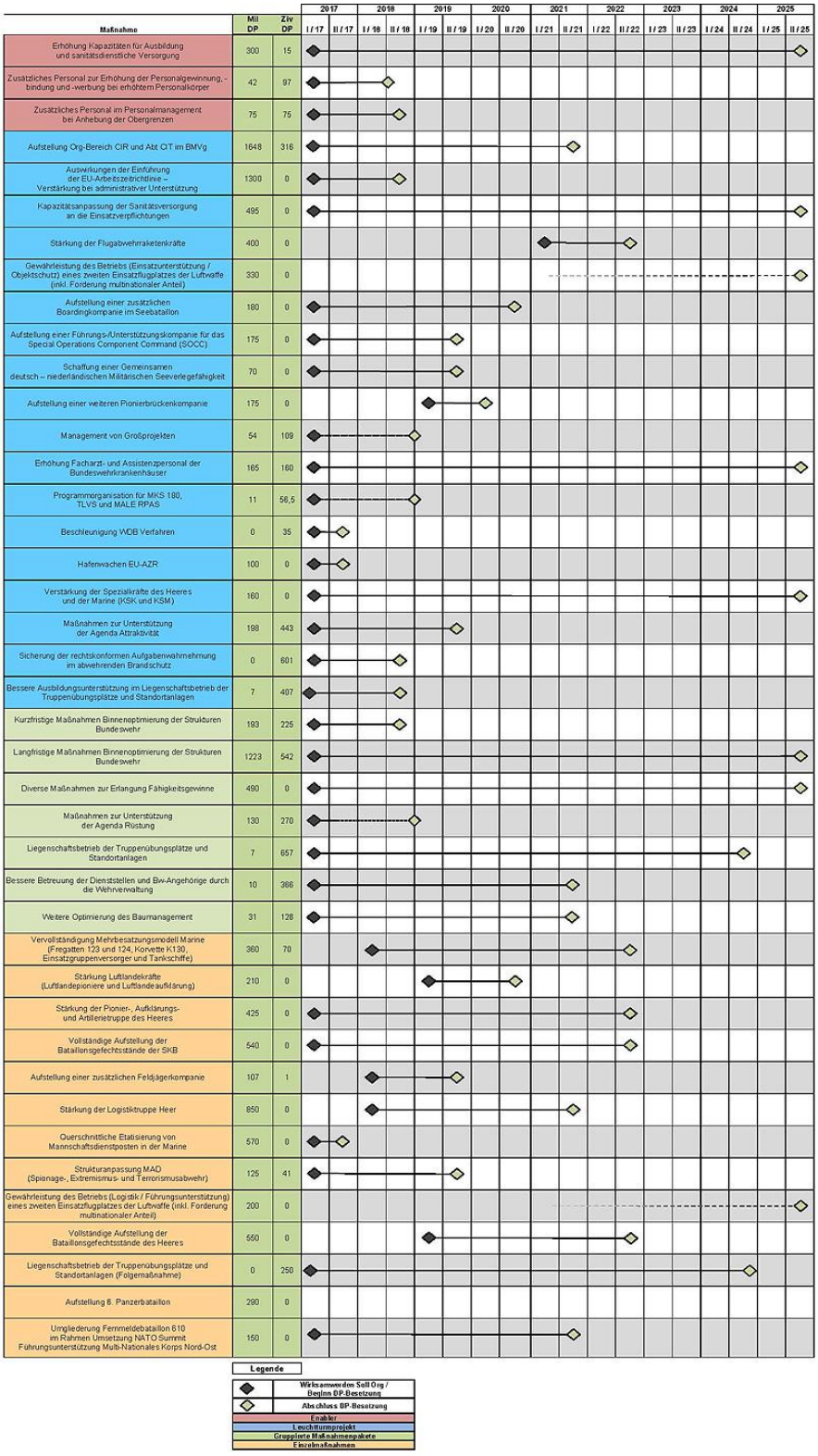
---

[6] http://www.bmvg.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NmU2ODYyNzc2MzY5NzMyMDIwMjAyMDIw/Abschlussbericht%20Aufbaustab%20CIR.pdf

[7] http://www.bmvg.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NmU2ODY1NzE3NTYxNmMyMDIwMjAyMDIw/Folien%20CIR%20Online.pdf

Anhang

Abbildung 1: Aufschlüsselung des Personalumbaus im Rahmen des Tagesbefehls vom 10.5.2016, Quelle: augengeradeaus.net[8]



[8] http://augengeradeaus.net/2016/05/es-ist-zeit-fuer-die-bundeswehr-wieder-zu-wachsen/