Bundesministerium der Verteidigung

Abschlussbericht
Aufbaustab Cyber- und Informationsraum

Empfehlungen
zur Neuorganisation von
Verantwortlichkeiten, Kompetenzen und Aufgaben
im Cyber- und Informationsraum
sowie
ergänzende Maßnahmen zur Umsetzung der
Strategischen Leitlinie Cyber-Verteidigung

April 2016

Inhaltsverzeichnis

1. Zusammenfassung

Staat, Wirtschaft und Gesellschaft sind in einer zunehmend vernetzten, digitalisierten Welt für Angriffe im Cyber- und Informationsraum (CIR) verwundbarer geworden. Diese digitale Verwundbarkeit der Gesellschaft haben sich in den letzten Jahren staatliche und nichtstaatliche Akteure – insbesondere im Rahmen der hybriden Kriegsführung – zu Nutze gemacht. Die mögliche Anonymität von Angriffen (Attributionsproblematik) und die kostengünstigen Möglichkeiten zur asymmetrischen Wirkung haben Cyber-Angriffe und Maßnahmen im Informationsumfeld zu einem wirkungsvollen Mittel gemacht - häufig um Ziele unterhalb der Schwelle eines militärischen Angriffs durchzusetzen. Die zunehmend komplexeren Angriffe erfordern den Ausbau der staatlichen Handlungsfähigkeit zum Schutze unseres demokratischen Systems und seiner wirtschaftlichen Grundlagen. Die NATO behandelt den Cyber- und Informationsraum deshalb als einen eigenen Operationsraum, viele Partnerländer haben eigene Cyber-Fähigkeiten in eigenen Organisationsformen ausgeprägt.

Auch die Bundeswehr muss ihren Beitrag für die Sicherheitsarchitektur in Deutschland ausbauen und sich auf die neuen Bedrohungen aus dem Cyber- und Informationsraum einstellen. Die technische Weiterentwicklung von einfachen Viren hin zu komplexen, schwer erkennbaren Attacken (Advanced Persistant Threats) stellt einen Qualitätssprung in der Bedrohungslage dar. Cyber-Angriffe auf Staaten und Kritische Infrastrukturen sind schon lange keine Fiktion mehr, sondern Realität. Zahlreiche Vorfälle in ähnlich entwickelten und digitalisierten Partnerländern und -streitkräften in den letzten Jahren belegen dies. Der Ausbau von Cyber-Fähigkeiten ist daher ein essentieller Beitrag zur gesamtstaatlichen Sicherheitsvorsorge und bietet zusätzliche Handlungsoptionen für Konfliktverhütung und Krisenbewältigung einschließlich der Begegnung hybrider Bedrohungen.

Die Bundeswehr als zunehmend digitalisierte Großorganisation muss sich deshalb für die Chancen der Digitalisierung und die Bedrohungen des Cyber- und Informationsraums organisatorisch aufstellen. Der Aufbaustab CIR empfiehlt folgende **organisatorische Maßnahmen**:

- Einrichtung einer **Abteilung Cyber/ IT (CIT) im Bundesministerium der Verteidigung** (BMVg) zum 1. Oktober 2016 (Grundbefähigung)
- Aufstellung eines **militärischen Organisationsbereichs** für den **Cyber- und Informationsraum** mit einer Inspekteurin bzw. einem Inspekteur an der Spitze zum 1. April 2017 (Erstbefähigung)

In der **Abteilung CIT im BMVg** in Berlin und in Bonn wird unter der Führung einer oder eines Ressort Chief Information Officer (Ressort-CIO) die Verantwortung für die Themen Cyber und IT „in einer Hand“ gebündelt (IT-Architekt). Der oder die Ressort-CIO verantwortet die Bereiche Cyber-/ IT-Governance und IT-Services/ Informationssicherheit sowie die unternehmerische Steuerung der Bundeswehr Informationstechnik GmbH (BWI). Diese Abteilung CIT folgt dem Prozessgedanken “PLAN, BUILD und RUN“. Die Bündelung der Kompetenzen für IT auf Abteilungsleiterebene soll so der stei-

genden Relevanz von IT und Digitalisierung Rechnung tragen und die Modernisierung der Bundeswehr in der Informationstechnologie schlagkräftig vorantreiben.

Mit dem Aufbau des **militärischen Organisationsbereiches CIR** soll der Cyber- und Informationsraum als Operationsraum bzw. militärische Dimension angemessen abgebildet werden. Zugleich wird damit der besonderen Schwerpunktsetzung innerhalb der NATO und der EU zu diesem Aufgabenbereich Rechnung getragen. Im neuen Kommando (Kdo) CIR in Bonn werden unter Führung der Inspekteurin bzw. des Inspekteurs die Aufgaben Cyber, IT, Militärisches Nachrichtenwesen, Geoinformationswesen und Operative Kommunikation gebündelt und aus einer Hand truppendienstlich und fachlich geführt. Dazu wandern in einem ersten Schritt ca. 13.700 Dienstposten mit ihren Aufgaben zum Organisationsbereich CIR. Darüber hinaus werden ca. 300 Dienstposten für die Führungsfähigkeit des KdoCIR, die Aufstellung eines Zentrum Cyber-Sicherheit der Bundeswehr und die Stärkung der Aufgabe Computer Netzwerk Operationen herangezogen. Für das Kommando des Organisationsbereichs wird eine schlanke Startaufstellung empfohlen. Die bisherigen Standorte bleiben erhalten. Weitere Fähigkeiten werden auf der Zeitachse auf- und ausgebaut.

Mit der organisatorischen Weiterentwicklung auf der Ebene BMVg und dem Organisationsbereich CIR kann die Bundeswehr die entscheidenden Weichen für eine stärker IT-getriebene Modernisierung und die Aufwertung des Cyber- und Informationsraums als militärische Dimension stellen. Effizientere und schlagkräftigere Strukturen sind eine wesentliche und notwendige Voraussetzung für konkrete Verbesserungen wie schnellere Beschaffungsprozesse, einheitliche Strategien und harmonisierte Architekturen.

Um neben der organisatorischen Weiterentwicklung auch in der Substanz bereits Fortschritte zu machen und die Modernisierung voranzubringen, empfiehlt der Aufbaustab **ergänzende Maßnahmen** auch zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung. Diese Maßnahmen zielen auf verschiedenste Bereiche wie Personal (z.B. dynamische Werdegangsmodelle), Rekrutierung und Ausbildung (z.B. Cyber-Security Studiengang an der UniBw München), den Ausbau der „Cyber Awareness“ in der Bundeswehr (z.B. Cyber-Hygiene Check-Up) und die ressortübergreifende Kooperation im Cyber-Raum (z.B. Dialog mit dem Bundesministerium des Innern).

2. Strategischer Kontext

Die Digitalisierung und Cyber-Bedrohung vollzieht sich mit exponentieller Geschwindigkeit und ist auch für die Streitkräfte nicht aufzuhalten. Schlagwörter sind: Industrie 4.0, Big Data, Predictive und Advanced Analytics. Moderne Gesellschaften und Volkswirtschaften sind in hohem Maße auf die gesicherte und freie Nutzung des grenzenlosen Cyber- und Informationsraumes (CIR)[1] angewiesen. Durch die zunehmende digitale und informationsseitige Vernetzung von Staat, Wirtschaft und Gesellschaft sind diese jedoch auch für Angriffe im Cyber- und Informationsraum verwundbarer geworden.

Vor dem Hintergrund der hybriden Kriegsführung gilt es, Bedrohungen der Zukunft zu verstehen, aber auch die Chancen der Zukunftstechnologien bereits heute für die Bundeswehr zu erkennen.

Abbildung 1: Illustration militärischer Entwicklungssprünge

In den letzten Jahren haben sich viele staatliche und nichtstaatliche Akteure die Möglichkeiten des Cyber- und Informationsraums zu Nutze gemacht:

- Schon heute sind Cyber-Angriffe fester Bestandteil konventioneller Operationen von Streitkräften oder Nachrichtendiensten, so zu beobachten in der Georgien-Krise 2008, der hybriden Kriegsführung in der Ukraine, aber auch bei dem Hacker-Angriff auf das Netz des Deutschen Bundestages.
- Cyber-Technologien sind kostengünstig und effektiv – erzielen also asymmetrische Wirkung (Stichwort sind DDoS-Attacken, APTs, backdoors, hacktivists und Cyber-Armeen). Häufig um Ziele - unterhalb der Schwelle eines militärischen Angriffs - durchzusetzen.
- Cyber-Angriffe umfassen Spionage, Informationsmanipulation, mögliche Cyber-Terrorakte bis hin zu groß angelegten Sabotage-Attacken bspw. bei Kritischer Infrastruktur.
- Proliferation und exponentiell schnelle IT-Entwicklung verstärken den Trend, dass die Bedrohung überproportional zur Fähigkeit zur eigenen Verteidigung wächst.
- Cyber-Angriffe sind geplant und auf ein Ziel ausgerichtet. Die Akteure hinter den Angriffen haben klare Interessen, sind aber im Schutze des World Wide Web schwierig zu identifizieren. Die eindeutige Attribution von Angriffen bleibt herausfordernd und technisch anspruchsvoll.
- Das Wissen ist zunehmend breiter zugänglich. Der Weiterverbreitung von Schadprogrammen ist äußerst schwierig Einhalt zu gebieten. Cyber-Mittel stärken asymmetrische Kräfte. Das hebt die Bedrohung auf eine neue Qualitätsstufe.

[1] Der Cyber- und Informationsraum ist ein komplexes System und vereint in sich den Cyber-Raum, das Elektromagnetische Spektrum und das Informationsumfeld.

Nicht nur die Quantität, vor allem die Qualität der Bedrohung hat sich spürbar gewandelt.

- Die Entwicklung von einfachen Viren hin zu komplexen, schwer erkennbaren Attacken (Advanced Persistant Threats – APT) stellt einen Qualitätssprung dar. Es werden im Schnitt über 200 Tage benötigt, einen APT zu erkennen und in der Regel dauert es mehr als einen Monat, das Problem zu beheben.
- Solche Cyber-Angriffe auf Staaten und Kritische Infrastrukturen sind schon lange keine Fiktion mehr sondern Realität. Bekannte Beispiele sind:
    - o der „STUXNET-Angriff“ mit physischen Schäden an einer iranischen Uranzentrifuge (2010),
    - o der „OPM-Breach“ mit einem Datenabfluss in den USA von ca. 18 Millionen personenbezogener Daten von Staatsangestellten (2014/2015),
    - o der „Bundestaghack“, mit Schadsoftware auf Rechnern des Bundestags (2015).
- Zwar können vereinzelt Vorgehensmuster erkannt werden. Dennoch sind die modernen Hochwertangriffe meist auf das jeweilige Zielsystem maßgeschneidert.

So hat sich der CIR zu einem internationalen und strategischen Handlungsraum entwickelt, der sich jedoch klassischen Kategorien entzieht.

- 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.
- Die Schwierigkeit der Attribution, also der zweifelsfreien Zurückführung von Angriffen auf Verursacher, verstärkt die gefühlte Grenzenlosigkeit des Cyber-Raums.
- Gleichzeitig sind in den letzten Jahren große Fortschritte sowohl bei technischer Attribution als auch in völkerrechtlichen Fragen und vertrauensbildenden Maßnahmen erzielt worden.

Für die Bundeswehr bedeutet es, dass sie den Selbstschutz einer zunehmend digitalisierten Großorganisation sicherstellen muss. Waffensysteme sind heute schon mehr Software als Hardware, im Eurofighter sind z.B. rund 100 km Kabel und 80 Computer verbaut.

Die Funktionsfähigkeit der Bundeswehr ist somit entscheidend von zeitgerechten und verlässlichen Informationen abhängig. Deswegen kommt der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen eine entscheidende Bedeutung zu.

In keinem anderen Handlungsfeld sind die innere und äußere Sicherheit so verflochten und daher nur ganzheitlich und gesamtstaatlich zu gewährleisten. In der aktuellen Cyber-Sicherheitsstrategie für Deutschland vom Februar 2011 stehen zivile Ansätze und Maßnahmen im Vordergrund. Das Bundesministerium des Innern (BMI) erarbeitet derzeit federführend in Zusammenarbeit mit allen Ressorts die neue Cyber-Sicherheitsstrategie für Deutschland. Gleichzeitig arbeiten Auswärtiges Amt

(AA), BMI und BMVg im Kontext des Weißbuchs eng abgestimmt an der Gestaltung der gemeinsamen Cyber-Sicherheitsarchitektur – vom Völkerrecht zur Verteidigung.

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.
- Verteidigungsaspekte sind originäre Aufgaben von BMVg und Bundeswehr.

Die Bundeswehr muss daher die eigene Handlungsfähigkeit im CIR sicherstellen und zukünftig einen an Bedeutung zunehmenden Beitrag zur gesamtstaatlichen Sicherheitsvorsorge leisten.

Gemeinsam gilt es, die gesamte Kette von Prävention zu Reaktion sowie von einfachen bis komplexen Angriffen zu beherrschen:

- Zur Sicherung der inneren Sicherheit bedarf es bspw. der Steigerung der allgemeinen „Cyber-Hygiene“ – also der erhöhten „Cyber-Awareness“ und „Cyber-Resilienz“ bei Bürgern, Wirtschaft und natürlich auch beim Staat. Hier setzen die unabdingbaren Maßnahmen des BMI zur Steigerung der IT-Sicherheit und des Grundschutzes an.
- Gleichzeitig muss die Bundeswehr auch für die neue Qualität von Cyber-Hochwertangriffen gerüstet sein, gegen die einfache Maßnahmen wie Firewalls und Detektionsfähigkeiten nicht ausreichen; gerade weil die Bundeswehr ein solches Hochwertziel für staatliche wie nichtstaatliche Organisationen ist.

Dabei gelten für den Einsatz von Streitkräften im Cyber-Raum stets die gleichen rechtlichen Voraussetzungen wie beim Einsatz anderer Fähigkeiten: Es gibt keinen Einsatz von Cyber-Kräften ohne entsprechende Einsatzmandatierung im Sinne des Parlamentsbeteiligungsgesetzes durch den Deutschen Bundestag.

Um der erheblichen Bedrohung im CIR zu begegnen, haben andere Nationen bereits in den vergangenen Jahren eigene Budgets oder Investitionsprogramme für den Cyber-Raum aufgelegt und verantwortliche Cyber-Kommandos aufgestellt, die den Aufbau und die Weiterentwicklung geeigneter Fähigkeiten vorantreiben.

Vielen Nationen ist gemein, dass das Thema Cyber-Verteidigung immer in einem gesamtstaatlichen Kontext eingebunden ist, zur Fähigkeitssteigerung über die nächsten Jahre erhebliche Anstrengungen im finanziellen und personellen Bereich unternommen werden, die Einbeziehung der Wirtschaft sowie der Wissenschaft einen großen Stellenwert besitzt und personelle Ressourcen durch Rückgriff auf eine Cyber-Reserve im Bedarfsfall schnell und effizient aufgestockt werden sollen. Ebenfalls breites Verständnis ist, dass zur Durchführung wirkungsvoller Cyber-Maßnahmen immer defensive und offensive Fähigkeiten erforderlich sind.

Darüber hinaus halten sich einzelne Staaten die Option offen, im Rahmen der Abschreckung das komplette Spektrum militärischer Mittel gegen Cyber-Angriffe einzusetzen.

Der dargestellte strategische Kontext zeigt die militärische Relevanz des CIR als eigene Dimension neben Land, Luft, See und Weltraum auf. Dieser ist umfassend Rechnung zu tragen.

3. Handlungsrahmen der Untersuchung

3.1 Auftrag und Auflagen

Der Tagesbefehl von Frau Bundesministerin der Verteidigung vom 17. September 2015 setzte folgenden Rahmen:

„Der Aufbaustab wird erstens einen Entwurf für ein neues, eigenständiges Org-Element Cyber/IT im Ministerium konzipieren. Alle Cyber/IT relevanten Aufgaben werden künftig in dieses Org-Element überführt und wo notwendig verstärkt.

Der Aufbaustab wird zweitens die Zusammenführung der Expertise im nachgeordneten Bereich steuern. Um dort die militärischen Fähigkeiten zu stärken, wird ein neuer herausgehobener Organisationsbereich für den "Cyber- und Informationsraum" in der Bundeswehr eingerichtet, der dem Ministerium unmittelbar nachgeordnet ist. Ziel ist es, dass die betroffenen Dienststellen an ihren Standorten unter einem Cyber- und Informationsraum Kommando (CIRK) zusammengefasst werden.“

Dabei waren folgende Randbedingungen bzw. Auflagen zu berücksichtigen:

- Die vorgeschlagenen Maßnahmen sollen zur **Umsetzung der „Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg“** vom 16. April 2015 beitragen.
- **Zuständigkeiten sind eindeutig zu regeln**, es soll eine Ansprechpartnerin bzw. ein Ansprechpartner auf der jeweiligen Ebene (BMVg, nachgeordneter Bereich) ressortübergreifend und international zuständig sein.
- **Das System Militärisches Nachrichtenwesen** mit seinen gesetzlichen Regelungen und das Verhältnis Militärisches Nachrichtenwesen, Bundesnachrichtendienst und Militärischer Abschirmdienst **stehen nicht zur Disposition**.
- Es sind **Chancen zu nutzen, die Kooperation mit Wissenschaft und Wirtschaft zu intensivieren,** Reservedienstleistende und Zivilpersonal sind einzubinden.
- Das **Stationierungskonzept ist grundsätzlich nicht zu verändern**, d.h. nach Möglichkeit kaum Änderung am Dienstpostenumfang der Standorte betroffener Dienststellen.
- Die vorgeschlagenen Maßnahmen müssen im **Einklang mit der „Agenda Attraktivität“ und der „Agenda Rüstung“** stehen.

3.2 Erfolgsfaktoren und Kriterien

Der dargestellte Auftrag und die Auflagen erfordern die Einleitung eines Veränderungsprozesses. Der Aufbaustab CIR hat hierzu die Strukturen und Prozesse analysiert und für die notwendige Bewertung den Nutzen, insbesondere hier den Zugewinn an militärischen Fähigkeiten, die technologischen Innovationsfähigkeit und personelle Attraktivität gegen den Aufwand, also den materiellen und personellen Ressourcen sowie dem notwendigen Veränderungsumfang abgewogen. Konkret wurden diese Faktoren wie folgt berücksichtigt:

Nutzen der organisatorischen Weiterentwicklung:

Fähigkeitsaufwuchs als Erfolgsfaktor schließt erkannte Lücken und verbessert das Zusammenwirken der Kräfte in der Dimension CIR. Mehrwerte für den CIR sind in erster Priorität durch Straffung der Prozesse und Strukturen zu erzielen. In zweiter Priorität kann die Stärkung von Kräften für den Fähigkeitsaufwuchs betrachtet werden, bei gleichzeitiger Berücksichtigung der auf der Zeitachse zur Verfügung stehenden Ressourcen.

Innovationsfähigkeit als Erfolgsfaktor schafft die Voraussetzungen frühzeitig Trends zu erkennen und zu nutzen, bspw. durch die Straffung der Strukturen, klare Adressierbarkeit und Sichtbarkeit nach innen und außen. Die am Markt entstehenden Innovationen sollen so rasch erkannt, bewertet und schnellstmöglich zur Verfügung gestellt werden. Die Abbildung an einer zentralen Stelle und vor allem die enge Verzahnung mit Wissenschaft, Industrie und Wirtschaft stärken die Innovationsfähigkeit für den CIR.

Attraktivität bezieht sich auf die Arbeitgeberattraktivität für potenzielle Bewerberinnen und Bewerber und die Zufriedenheit und Identifikation des bestehenden Personals. Die Teilhabe am Aufbau eines neuen Organisationsbereiches, der militärische Risiken und Bedrohungen zukunftsweisend begegnet, führt zur Steigerung der Attraktivität insbesondere durch entstehende neue Perspektiven. Der herausgehobene Organisationsbereich als Heimat für hochspezialisiertes Personal und Binnenstrukturen mit spezifischen Karrierepfaden führen zu einer hohen Arbeitgeberattraktivität. Einher gehen die deutliche Wahrnehmung nach innen und außen sowie die Assoziation des neuen Organisationsbereiches mit Zukunftstechnologien und innovativen Perspektiven.

Aufwand der organisatorischen Weiterentwicklung:

Ressourcen beziehen sich auf Personalobergrenzen, Personalverfügbarkeit – insbesondere bei Spezialisten – und den Aufwuchs an Spitzendienstposten. Sie stellen den Rahmen für strukturelle Änderungen. Das Stationierungskonzept ist vorgegeben. Die verfügbare Infrastruktur an den betroffenen Standorten begrenzt ggf. den Aufwuchs von Organisationselementen.

Veränderungsumfang als Kriterium misst, wie umfangreich die strukturellen Veränderungen sind und wie schnell diese umgesetzt werden können. Veränderungen müssen das Leistungsvermögen der Bundeswehr verbessern. Die Sicherstellung der Einsätze darf zu keinem Zeitpunkt beeinträchtigt werden.

Der Erfolg der Umstrukturierung ist gleichermaßen abhängig von einem geringen Veränderungsumfang, der Limitierung durch die zugewiesenen Ressourcen, der schnellen Umsetzbarkeit, der Erhöhung der Attraktivität sowie dem erreichten Fähigkeitsaufwuchs.

3.3 Ablauf und Meilensteine

Die Untersuchungen, die den Handlungsempfehlungen zugrunde liegen, wurden in einer Analyse- sowie Erarbeitungs- und Bewertungsphase mit nachfolgend dargestellten, wesentlichen Meilensteinen durchgeführt.

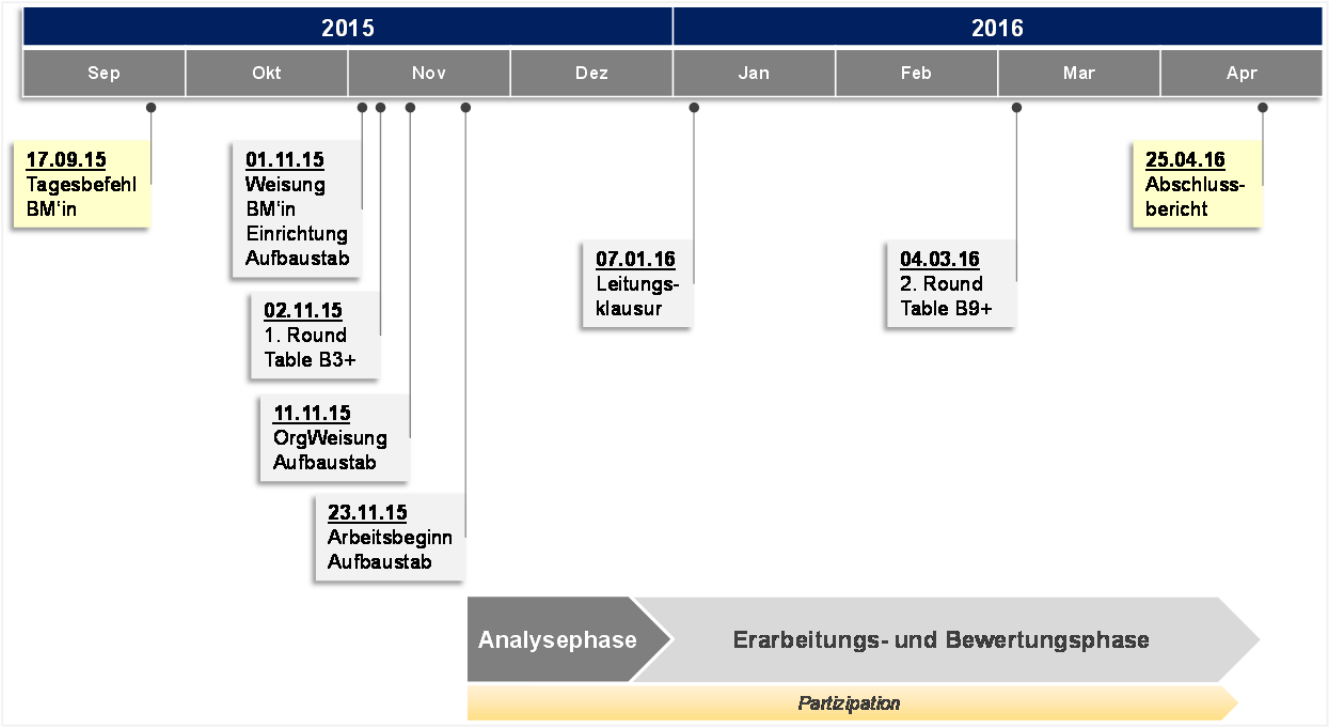

Abbildung 2: Zeitplan der Arbeiten Aufbaustab CIR

In der **Analysephase** erfolgte die Sammlung von Daten und Informationen, auf deren Basis der strategische Kontext und bestehende Defizite untersucht wurden. Des Weiteren wurden die unter Kapitel 3.2 dargestellten Erfolgsfaktoren und Kriterien als Maßstab für eine fundierte Entscheidungsfindung definiert. Hierbei trugen auch die Erfahrungswerte von Partnernationen und befreundeten Streitkräften bei, die sich aus dem Austausch mit Experten in den USA, im Silicon Valley und in Israel ergaben.

In der anschließenden **Erarbeitungs- und Bewertungsphase** wurden auf Basis der vorher festgelegten Erfolgsfaktoren und Kriterien Zielbilder für die neuen Organisationselemente entwickelt. Hierbei

wurde die vorhandene Kompetenz und Erfahrung der Bundeswehr und des BMVg systematisch eingebunden. In Workshops mit betroffenen Truppenteilen und Dienststellen wurden die Zielbilder auf Plausibilität, Vollständigkeit und Widerspruchsfreiheit geprüft. Die im weiteren Verlauf verfeinerten Zielbilder wurden im Rahmen eines zweiten Round Tables der Ebene B9+ vorgestellt. In diesem Zusammenhang konnten weitere wichtige Inputs aufgenommen werden.

Parallel wurden die **beteiligten Organisationsbereiche durchgängig in die Arbeiten einbezogen**. Neben Informationsveranstaltungen und Workshops wurden in persönlichen Gesprächen alle St**akeholder** im BMVg und im nachgeordneten Bereich eingebunden. Die Arbeit des Aufbaustabes wurde zudem durch ein Informationsangebot im Intranet begleitet.

Die konsolidierten Ergebnisse der Analyse-, Erarbeitungs- und Bewertungsphase sind in diesen Abschlussbericht eingeflossen.

4. Ableitungen aus den Vorgaben und Rahmenbedingungen

In Umsetzung der „Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg“ vom 16. April 2015 soll die Bundeswehr im Cyber-Raum zukunftsfähig aufgestellt und darüber hinaus zu einer verbesserten Operationsführung im CIR befähigt werden.

Wesentliche Voraussetzung dafür ist eine Bündelung von Zuständigkeiten und Kompetenzen und damit eine adäquate organisatorische Abbildung sowohl im BMVg als auch im nachgeordneten Bereich. Daneben ergeben sich weiterführende Konsequenzen, die begleitende Maßnahmen erfordern, um die angestrebte Wirkung der Organisationsänderungen erreichen zu können:

- wesentliche Aktivitäten in der Abteilung CIT und im Organisationsbereich CIR sind in Leistungsprozessen (LP) abzubilden,
- agile Planungsprozesse für Cyber/ IT sind zu schaffen,
- die IT-Sicherheit ist zur Informationssicherheit weiterzuentwickeln,
- die Bundeswehr ist im Bereich CIR weiter zu professionalisieren.

Auf Basis der dargestellten Ableitungen werden Handlungsempfehlungen für die organisatorische Gestaltung und erste ergänzende Handlungsempfehlungen zur Umsetzung der Strategischen Leitlinie in den Kapiteln 5 und 6 gegeben.

4.1 Eigenständiges Organisationselement im BMVg für den Bereich Cyber/ IT

Die heute im BMVg verteilten Verantwortlichkeiten für Cyber/ IT verursachen Schnittstellenverluste und beeinträchtigen die Handlungs- und Reaktionsfähigkeit. Der technischen Weiterentwicklung und Innovationgeschwindigkeit kann nicht hinreichend Rechnung getragen werden. Daher sind die zersplitterten, vielfältigen Handlungslinien und Kommunikationsbeziehungen im Bereich Cyber/ IT bereits auf der Ebene BMVg zu bündeln. Dadurch wird die IT in der Bundeswehr effektiver aufgestellt und der Weg hin zu einer einheitlichen IT-Architektur beschritten.

Für die Realisierung ist dafür die Rolle der bzw. des Chief Information Officer des Ressorts (Ressort-CIO) dergestalt im BMVg abzubilden, dass dieser bzw. diese neben den ressorteigenen Zielen (bspw. querschnittliche IT-Modernisierung der Bundeswehr) auch die ressortübergreifenden IT-Vorgaben der Bundesregierung durchsetzungsfähig umsetzen kann. Dazu ist das neue, eigenständige Organisationselement Cyber/ IT im BMVg als Abteilung unter Leitung des oder der Ressort-CIO zu etablieren. Diese bzw. dieser steuert sowohl die technologische/ technische Weiterentwicklung von Cyber/ IT[2], einschließlich der IT-Architekturen, als auch Einsatz, Betrieb und Schutz der IT in der Bundeswehr sowie die BWI als Inhouse-Gesellschaft. Ihm oder ihr muss dafür ein mit der Gesamtplanung der Bundeswehr harmonisiertes Budget zur Wahrnehmung seiner bzw. ihrer

[2] Dies schließt eine Weisungsbefugnis des bzw. der Ressort-CIO u.a. gegenüber BAAINBw im Rahmen seiner Zuständigkeit mit ein.

Planungsverantwortung eingeräumt werden. Durch die Etablierung des oder der Ressort-CIO auf Abteilungsleiterebene im BMVg wird darüber hinaus die ministerielle Ansprechbarkeit national und international auf angemessener Ebene gebündelt sichergestellt.

Die Verantwortung für die Sicherstellung der einsatzbezogenen Bewertungen für den CIR ist durch die beabsichtigte Bündelung nicht zu verändern. Diese ist auch weiterhin durch die Abteilung Strategie und Einsatz wahrzunehmen, um die Kohärenz von der ministeriellen Ebene bis in die Einsätze aufrecht zu erhalten.

4.2 Eigenständiger militärischer Organisationsbereich für die Dimension Cyber- und Informationsraum

Der beschriebenen herausgehobenen sicherheitspolitischen und militärischen Bedeutung des CIR als militärische Dimension ist organisatorisch, strukturell zukunftsfähig und nach außen deutlich sichtbar durch die Einrichtung eines eigenständigen militärischen Organisationsbereiches Rechnung zu tragen. Die Inspekteurin bzw. der Inspekteur des Organisationsbereiches CIR kann sich ausschließlich auf die Dimension CIR konzentrieren und die Führung aus einer Hand sicherstellen.

Mit einer Inspekteurin oder einem Inspekteur kann darüber hinaus ein durchsetzungsfähiger und eindeutig erkennbarer Point of Contact (PoC) für die Bundeswehr etabliert werden, der zukünftig die zu intensivierende nationale und internationale Zusammenarbeit aus einer Hand und auf Augenhöhe sicherstellen kann. Die absehbar kontinuierlich steigende Bedeutung und Dynamik der Dimension CIR und die intensivierte Zusammenarbeit erfordern diese Fokussierung und Handlungsfähigkeit.

Zu diesen Handlungsfähigkeiten gehört eine auf den Organisationsbereich abgestimmte Personalentwicklung und -führung für militärisches und ziviles Personal, die von der Inspekteurin bzw. vom Inspekteur CIR als Bedarfsträger effektiver mitgestaltet werden kann.

Zur Aufstellung des Organisationsbereiches CIR sind vorhandene Ressourcen entsprechend ihres fachlich-inhaltlichen Zusammenhangs zusammenzuführen. Dadurch werden vor allem

- die notwendige, stärkere operationelle Nutzung der Dimension CIR,
- die Steigerung der Attraktivität zur Gewinnung und Bindung dringend benötigter Fachkräfte und
- die dynamische Zukunfts- und Weiterentwicklung der zugehörigen Fähigkeiten

ermöglicht.

Die Bundeswehr wird mit einem neuen militärischen Organisationsbereich CIR wirkungsorientierte Aktivitäten im CIR als militärische Operation aus Deutschland heraus und in Einsätzen in Zusammenarbeit mit bewährten Strukturen aus einer Hand führen und unterstützen können. Die Dimension CIR kann durch die Aufstellung des militärischen Organisationsbereiches CIR adäquat als Operationsraum erschlossen werden.

4.3 Dimension Cyber- und Informationsraum als Operationsraum

Der CIR ist eine eigene Dimension im Kontext der hybriden Kriegsführung – aber immer auch eng verbunden mit den Operationsräumen in den Dimensionen Land, Luft, See und Weltraum. Er unterliegt daher mit seinen spezifisch zugeordneten Kräften auch einer eigenständigen Planung und Durchführung, die letztlich zu einem unterstützenden, komplementären oder auch substituierenden Einsatz bei Operationen führt. Ziel ist es, Informationsdominanz im Operationsraum zu erreichen, um Entscheidungsprozesse zu optimieren und Einsatzwirkung zu maximieren. Dazu ist der dauerhafte Schutz eigener Informationen sicherzustellen und das Gewinnen, Auswerten und Wirken auf gegnerische Informationen zu ermöglichen.

Kräfte und Mittel für Operationen im CIR werden im Wesentlichen durch den Organisationsbereich CIR bereitgestellt. Teilfähigkeiten verbleiben unverändert in ihren jeweiligen Teilstreitkräften/ Organisationsbereichen, können jedoch auch zu Operationen im CIR beitragen.

Operationen, die nur im CIR stattfinden, sind denkbar, jedoch sind die über den CIR erzielbaren Effekte grundsätzlich Teil einer streitkräftegemeinsamen Operation. Wesentlich hierfür ist die Bereitstellung von umfänglicher Beratungskompetenz für die militärische Truppenführerin oder den militärischen Truppenführer im Einsatz bzw. die Befehlshaberin oder den Befehlshaber Einsatzführungskommando der Bundeswehr/ Abteilungsleiterin oder Abteilungsleiter Strategie und Einsatz im BMVg.

Operationelle Aufgaben im Organisationsbereich CIR sind unter anderem:

- Gewährleisten von Informationssicherheit und Schutz des IT-Systems der Bundeswehr sowohl im Einsatzgebiet als auch in Deutschland im Sinne einer Dauereinsatzaufgabe,
- Beitragen zum Schutz kritischer Cyber/ IT-Infrastrukturen im Rahmen der gesamtstaatlichen Sicherheitsvorsorge,
- Erstellen einer umfassenden militärischen Nachrichtenlage sowie eines übergreifenden Cyber-Lagebildes und Beitragen zu einem gesamtstaatlichen Lagebild,
- Durchführen von Computer Netzwerk Operationen (CNO) im Cyber-Raum sowie Maßnahmen des Elektronischen Kampfes (EK) im elektromagnetischen Spektrum,
- Nutzen des Informationsumfeldes zur Erkennung von Propaganda und Desinformation in Krisengebieten,
- Teilhaben an der Meinungsbildung im Informationsumfeld der Interessengebiete der Bundeswehr[3] und in mandatierten Einsätzen.

Neben einer entsprechenden Abbildung in den relevanten Stäben ist dazu insbesondere in Anbetracht der internationalen Entwicklungen bei Partnern („Cyber-Kommandos“) und in der NATO („Cyber as a Domain“) für den Einsatz von Fähigkeiten die Entwicklung von entsprechenden Planungs-

[3] Im Einklang mit dem grundgesetzlichen Neutralitätsgebot des Staates.

und Einsatzverfahren wie auch das Vorhalten eines multinationalen Kommandoelements für den CIR erforderlich[4].

Durch die kontinuierliche Analyse des CIR, den umfassenden Schutz der eigenen IT-Systeme sowie die Bündelung der wesentlichen Fähigkeiten in einem militärischen Organisationsbereich unter einheitlicher Führung wird eine operationelle Nutzung des CIR ermöglicht. In Analogie zu der ungeteilten Verantwortung in den Dimensionen Land, Luft und See sind durch das Kommandoelement Operationen im CIR als Beitrag für die Gesamtoperation auszuplanen.

Gerade vor dem Hintergrund hybrider Bedrohungen (z.B. durch staatlich gesteuerte „Hacker-Angriffe“) können die Fähigkeiten der Bundeswehr zum Schutz des CIR zukünftig auch einen wesentlichen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge leisten.

4.4 Prozessuale Abbildung im Geschäftsbereich BMVg

Leistungsprozesse im Geschäftsbereich BMVg sind bestimmend für die Aufbau- und Ablauforganisation. Daher wurde parallel zur Erarbeitung von Lösungsvorschlägen analysiert, ob die existierenden Prozesse die Anteile Cyber/ IT und CIR adäquat abbilden. Da auf der derzeitigen Prozesslandkarte BMVg keine Abbildung der militärischen Aspekte eines Leistungsprozesses für den CIR vorgesehen ist und im nachgeordneten Bereich nur einzelne Ausschnitte des CIR betrachtet werden, wird zur Sicherstellung der ministeriellen Steuerung die Erstellung eines neuen Leistungsprozesses für Cyber/IT-Governance und Sicherstellung der Informationssicherheit sowie die Einbettung der militärischen Aspekte des Cyber- und Informationsraums in bestehende Leistungsprozesse empfohlen.

4.5 Agile Planungsprozesse für Cyber/ IT

Mit der organisatorischen Zusammenfassung von Zuständigkeiten und Kompetenzen im Bereich Cyber/ IT soll zukünftig unter anderem auch den schnellen Innovationszyklen der IT Rechnung getragen werden. Dazu bedarf es jedoch ergänzend auch optimierter und agiler Planungsprozesse für diesen Bereich.

IT ist beides: Teil des Gesamtsystems Bundeswehr und somit, bspw. in der Waffensystem-IT, eng mit der Planungsarbeit in der Rüstung verbunden, und gleichzeitig eigene Materialkategorie mit kürzeren Entwicklungszyklen und mehr marktverfügbaren Lösungen. Die Planungsprozesse hierfür müssen deshalb agiler umgesetzt werden. IT-Planung für marktverfügbare Lösungen muss einfacher ablaufen, als die Planung eines komplexen Waffensystems. Die Planungsprozesse für Embedded IT sollen sich deshalb am heutigen Planungsprozess nach IPP/ CPM (nov.) orientieren, andererseits aber in der reinen IT den Besonderheiten Cyber/ IT gerecht werden. Dabei sind zwei Ziele zu erreichen:

[4] Vergleichbar beispielsweise mit einem Component Command (CC) für andere Dimensionen.

- Die bzw. der Ressort-CIO trägt die Planungsverantwortung für alle IT-Projekte in ihrem bzw. seinem Verantwortungsbereich und verantwortet die übergreifende IT-Architektur der Bundeswehr sowie die Umsetzung der ressortübergreifenden IT-Vorgaben.
- Der oder die Ressort-CIO bewertet zukünftig alle Initiativen zu Cyber/ IT und verantwortet und steuert die Erstellung der zugehörigen Forderungsdokumente. Damit lassen sich durch strikte Straffung der Bearbeitungswege und Schwerpunktsetzung im eigenen Bereich – analog zu dem mit der IT-Strategie im Geschäftsbereich BMVg eingeführten Verfahren für Architekturprojekte – die Bearbeitungszeiten deutlich reduzieren (heute regelmäßig > 1 Jahr).

Der angepasste Prozess sieht zusätzlich vor, dass im Rahmen eines ersten Planungspanels[5] das Budget[6] der bzw. des Ressort-CIO unter anderem auf Basis der IT-Strategie des Geschäftsbereiches BMVg und der darin enthaltenen Ziele und Maßnahmen für den jeweils nächsten Planungszyklus festgelegt wird. In einem zweiten Planungspanel kann dieses an ggf. geänderte haushalterische Rahmenbedingungen angepasst werden. Wesentlicher Unterschied zum heutigen Verfahren ist, dass der Gesamtumfang des Budgets der bzw. des Ressort-CIO und mögliche erforderliche planerische Anpassungen in zwei festgelegten Planungspanels beschlossen werden. Unterhalb eines so festgelegten Budgetplatfonds setzt der bzw. die CIO die IT-Prioritäten der Bundeswehr. Dies trägt der Verantwortung der bzw. des Ressort-CIO und der Komplexität der Aufgabe Rechnung. Die Details sowie weitere Möglichkeiten zur Straffung des Verfahrens werden bis Ende 2016 ausgearbeitet.

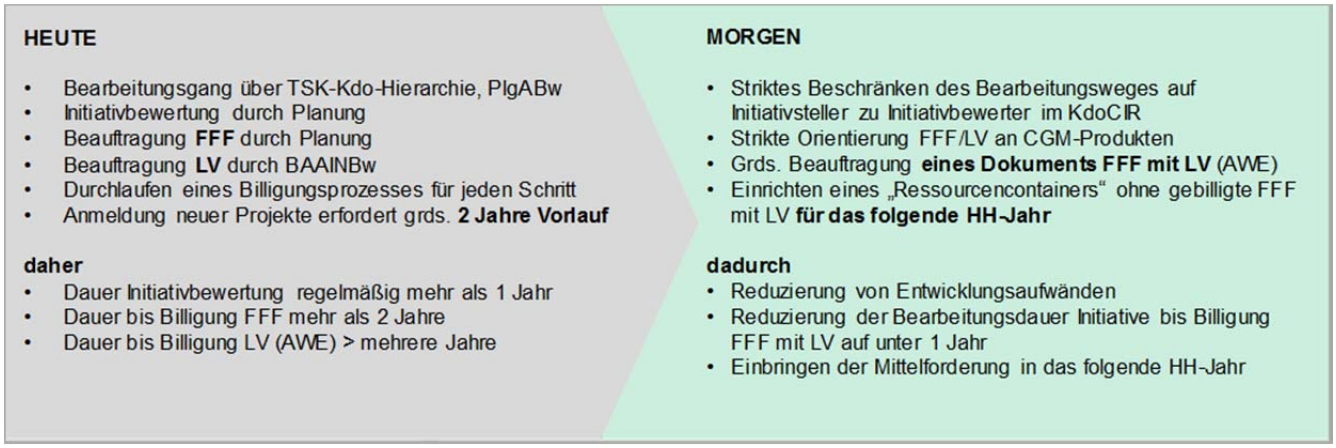

Abbildung 3: Beschleunigung der Einführung von IT

Neben dieser Modifikation des bisher bestehenden Prozesses müssen weitere Verfahren geschaffen werden, um auch das Ziel einer deutlichen Beschleunigung bei der Einführung („Monate statt Jahre“) von CGM-Produkten[7] zu erreichen. Dies spart Entwicklungszeit für aufwändige Speziallösungen, reduziert Kosten und ermöglicht damit eine schnellere Einführung von IT. Dazu wird die Einrichtung von

[5] Planungspanel: Mitglieder sind die beiden beamteten Sts, GenInspBw, AL Plg, AL HC und Ressort-CIO.
[6] Summe der durch die bzw. den Ressort-CIO priorisierten Maßnahmen und Projekte und deren Finanzbedarf.
[7] CGM: Commercial, Government, Military off the Shelf, d.h. Standard-Produkte, die verfügbar sind und nicht entwickelt werden müssen.

„Ressourcencontainern“ für die Anmeldung im Haushalt, die den Rahmen für die Beschaffung von zeitgemäßer Standard-IT setzen, jedoch den Abruf des konkreten Bedarfs an Umfang und Technologie sehr kurzfristig ermöglichen würden, angestrebt.

Die Einführung und Beschaffung von IT wird deutlich beschleunigt, damit diese nicht bereits mit Beginn der Nutzung veraltet ist. Auf dieser Basis wurde mit der Abteilung Planung ein angepasster Planungsprozess im Grundsatz abgestimmt. Details hierfür werden bereits ausgearbeitet.

4.6 Informationssicherheit

Aufgrund der umfassenden Bedeutung von Informationen im CIR muss auch deren Schutz neu ausgerichtet werden. Der Schutz von Informationen unter Berücksichtigung von Vertraulichkeit, Integrität und Verfügbarkeit (Schutzziele) beschränkt sich heute im Wesentlichen auf drei Bereiche:

- den Schutz der Informationstechnik (IT-Sicherheit),
- den Schutz von nationalen und internationalen Verschlusssachen (Geheimschutz),
- den Schutz personenbezogener Daten (Datenschutz).

Diese werden heute überwiegend als eigenständig betrachtet, beeinflussen sich jedoch – insbesondere bei der Verarbeitung und Übertragung von Informationen mittels technischer Verfahren – gegenseitig.

Aufgrund dieser Wechselwirkungen müssen die Schutzziele – im Gegensatz zur klassischen IT-Sicherheit – auf Basis einer ganzheitlichen Betrachtung der Informationssicherheit und unter Berücksichtigung nicht-technischer Aspekte ergänzt werden. Dabei sind zusätzliche Einflussfaktoren wie beispielsweise Personal, Prozesse und Compliance[8] zu berücksichtigen.

Ein übergreifendes Informationssicherheitsmanagement ist erforderlich, welches den Schutz von Informationstechnik (IT-Sicherheit) in den Schutz aller Informationen (Informationssicherheit) integriert. Dies wird in der Folge zu einer engeren Verzahnung von IT-Sicherheit, Geheimschutz und Datenschutz führen. Neben der Steigerung des Gesamtschutzes werden sich durch die organisatorische Zusammenführung auch wesentliche Synergieeffekte erzielen lassen.

4.7 Weitere Professionalisierung der Bundeswehr im Cyber- und Informationsraum

Damit der neue militärische Organisationsbereich CIR seine volle Wirkung entfalten und einen Mehrwert gegenüber den bisherigen Strukturen darstellen kann, sind sowohl das Personal weiter zu professionalisieren als auch die Strukturen und Verfahren insbesondere im Bereich Cyber/ IT weiter zu verbessern. Dies betrifft sowohl die Fort- und Weiterbildung der rund 20.000 Mitarbeiter und Mitarbeiterinnen, die bereits heute auf IT-nahen Dienstposten arbeiten, als auch die anderen Mitarbeiterinnen und Mitarbeiter, die in der zunehmend digitalen Bundeswehr mitwirken.

[8] Einhaltung gesetzlicher Vorschriften und betrieblicher Richtlinien.

Dies erfordert kompetentes Personal auf allen Ebenen in attraktiven Strukturen, das gut ausgebildet konkurrenzfähige technische Fähigkeiten für seine herausfordernden Aufgaben besitzt. Hierzu bedarf es entsprechender Ausbildungsmöglichkeiten auf allen Bildungsebenen (z.B. Fachausbildung, universitäre Ausbildung), adäquater Werdegänge und geeigneter Personalgewinnungs- und Bindungsmaßnahmen. Darüber hinaus ist eine zentrale Steuerung der Ausbildung und Personalentwicklung durch den Organisationsbereich Personal erforderlich.

Um technologisch den Anschluss an die schnelllebige IT-Branche nicht zu verlieren, müssen Innovationen, insbesondere in dem Schlüsselbereich Software, schnell verfügbar gemacht werden. Die Nutzbarkeit von technologischen Innovationen sollte durch Förderung der Cyber-/ IT- und Sicherheitsforschung gezielt vorangetrieben werden, um so die Umsetzung auch in militärisch nutzbare Technologien zu beschleunigen. Mittels eines aktiven Innovationsmanagements und in der Zusammenarbeit mit Industrie, Wirtschaft, Forschungseinrichtungen und Universitäten sollen externe Innovationen für die Bundeswehr nutzbar gemacht werden.

Eine wesentliche Säule für die Zukunftsfähigkeit der Bundeswehr im Cyber- und Informationsraum wird die Entwicklung und Versorgung nationaler Schlüsseltechnologien in ausgewählten Fähigkeiten zur Sicherung der digitalen Souveränität sein. Mit dem Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland vom 8. Juli 2015 wurden wesentliche Rahmenbedingungen für den Erhalt nationaler verteidigungsindustrieller Schlüsseltechnologien u.a. im Bereich Cyber definiert. In diesen Technologiebereichen sind die „erforderlichen Fähigkeiten und die Versorgungssicherheit der Bundeswehr sowie die Rolle Deutschlands als zuverlässigem Kooperations- und Bündnispartner technologisch und wirtschaftlich sicherzustellen, insbesondere im Rahmen auch zunehmend globalisierter Lieferketten“. Ausschließlich in der Erbringungsdimension Cyber wurden durch die Bundesregierung nationale Schlüsseltechnologien in allen vier Fähigkeitsdomänen der Bundeswehr identifiziert (Führung, Aufklärung, Wirkung und Unterstützung). Der Schwerpunkt in der Domäne Führung liegt in der Krypto-Technologie. Für den Erhalt und die Schaffung nationaler Schlüsseltechnologien gilt es im Bereich Cyber-Sicherheit einen Nukleus für eine enge Verzahnung mit Behörden, Forschung, Lehre, Industrie zu schaffen und damit innovative Technologien bzw. Start-Up-Unternehmen in den komplexen und derzeit noch langwierigen Beschaffungsprozess des öffentlichen Auftraggebers einzubinden. Hier gilt es nun im Dialog mit den zuständigen Ressorts und der Industrie neue Wege zu identifizieren, um die Zukunftsfähigkeit der Streitkräfte für den Bereich Cyber zu sichern.

Zur Bewertung der militärischen Nutzbarkeit von Innovationen ist eine entsprechende eigene Bewertungs- und Beratungskompetenz erforderlich. Noch vorhandene Kompetenzen im Bereich Softwareentwicklung sind daher zu erhalten, auszubauen und in einem organisatorischen Element für Softwarekompetenz zusammenzuführen.

5. Organisatorische Handlungsempfehlungen mit Mehrwerten

5.1 Abteilung Cyber/ IT im BMVg

Auf Basis der Auflagen, Ableitungen sowie Erfolgsfaktoren und Kriterien ist eine ministerielle Abteilung Cyber/ IT (CIT) im BMVg konzipiert worden, die sich durch folgende Mehrwerte auszeichnet:

- Die Abteilungsleiterin bzw. der Abteilungsleiter ist als Ressort-CIO zentraler ministerieller PoC des Ressorts in allen Cyber/ IT relevanten Angelegenheiten.
- Die ministerielle Steuerung sowohl der technologischen/ technischen Weiterentwicklung von Cyber/ IT als auch von Einsatz, Betrieb und Schutz der IT des Verteidigungsressorts erfolgt „aus einer Hand“.
- Die unternehmerische Steuerung der BWI wird durch die oder den Ressort-CIO wahrgenommen.

Diese Mehrwerte werden durch die nachfolgende organisatorische Ausgestaltung der ministeriellen Abteilung Cyber/ IT (CIT) im BMVg erzielt.

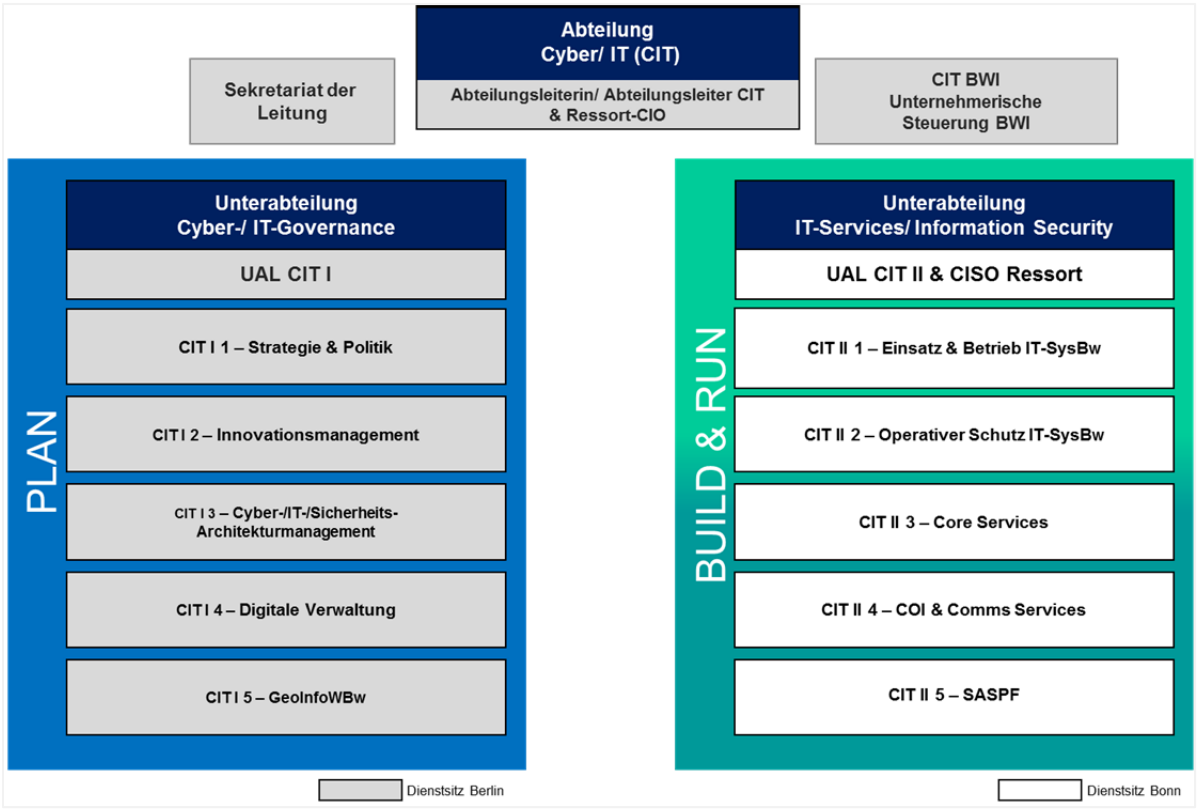

Abbildung 4: Abteilung Cyber/ IT im BMVg

Die Abteilung CIT zeichnet sich dadurch aus, dass die heute über mehrere Abteilungen verteilten Cyber/ IT-relevanten Aufgaben einschließlich deren Governance-Strukturen sowie die ministerielle Fachaufsicht gebündelt und wo erforderlich gestärkt sind. Den ressortübergreifenden Vorgaben der

Bundesregierung gemäß den Kabinettbeschlüssen zur IT-Steuerung des Bundes vom 5. Dezember 2007 sowie zur IT-Konsolidierung des Bundes vom 20. Mai 2015 folgend ist die neue Abteilungsleiterin bzw. der neue Abteilungsleiter CIT in seiner Rolle als Ressort-CIO mit zentraler Rahmenkompetenz für Cyber/ IT auszustatten. In Umsetzung sind dazu künftig insbesondere folgende Aufgaben wahrzunehmen:

- Entscheidungsbefugtes Vertreten von Cyber/ IT des Verteidigungsressorts nach außen (national und international),
- Gewährleisten der Übereinstimmung des IT-Einsatzes mit den politischen, strategischen und operativen Zielen des Ressorts und den IT-Festlegungen der Bundesregierung,
- Zukunfts- und Weiterentwickeln sowie Priorisieren von Bedarfsträgerforderungen für Cyber/ IT,
- Erlassen von zentralen Vorgaben für Konzeption, Realisierung, Nutzungssteuerung, Einsatz und Betrieb sowie Schutz der IT im Geschäftsbereich BMVg. Dies umfasst auch Vorgaben zur Standardisierung in allen Projekten mit IT-Anteilen (embedded IT) sowie für Geoinformationssysteme (GIS),
- Kontrollieren der Umsetzung von IT-Architekturen, IT-Standards, strategischen Zielvorgaben und der Festlegungen des IT-Rats,
- Bündeln der IT-Nachfrage des Ressorts und Fachaufsicht über die ressortinternen Anbieter von IT-Dienstleistungen einschließlich Wahrnehmung der Rolle des Gesellschafters der BWI nach deren Überführung in eine Inhouse-Gesellschaft,
- Konsolidieren der Erbringung von IT-Dienstleistungen innerhalb des Ressorts,
- Beteiligen bei Gesetzgebungsvorhaben des Ressorts, die Auswirkungen auf die Gestaltung der IT der öffentlichen Verwaltung haben,
- Gewährleisten der Informationssicherheit des Ressorts, mittels einer oder eines Ressort Chief Information Security Officer (CISO).

Zur Unterstützung der Wahrnehmung der Aufgaben der oder des Ressort-CIO sollte für die Leitung der neuen Abteilung CIT ein Sekretariat[9] der Leitung CIT vorgesehen werden, in dem u.a. Controlling-Aufgaben wahrgenommen werden.

[9] Verortung innerhalb der Abteilung CIT ist im Zuge der Feinausplanung zu prüfen.

Des Weiteren ist ein Immediatreferat[10] CIT BWI abgebildet, das die unternehmerische Steuerung der BWI nach deren Überführung in eine Inhouse-Gesellschaft wahrnimmt und die oder den Ressort-CIO bei der Wahrnehmung ihrer bzw. seiner Aufgaben als vorgesehener Gesellschafter der BWI unterstützt.

Dem Prinzip PLAN – BUILD – RUN folgend sind zwei Unterabteilungen mit folgenden Aufgaben ausgeplant:

Die Unterabteilung CIT I nimmt mit fünf Referaten im Schwerpunkt folgende Aufgaben der Cyber-/ IT-Governance (PLAN) wahr:

- Strategie und Politik, d.h.
  Cyber- und Digitalpolitik (einschließlich Frequenzpolitik), Cyber- und IT-Strategie, IT-Steuerung und IT-Konsolidierung Bund sowie nationale/ internationale Cyber-/ IT-Gremien und -Zusammenarbeit,
- Innovationsmanagement, d.h.
  CIO-Beitrag zur Finanzbedarfsanalyse und Mittelfristigen Zielsetzung, Zukunfts- und Weiterentwicklung von Cyber/ IT-Fähigkeiten, IT-Innovationsmanagement sowie Forschung und Technologie,
- Cyber-/IT-Architekturmanagement, d.h.
  Erstellung einer Cyber-/ IT-Architektur sowie einer IT-Sicherheitsarchitektur und -policy, Priorisierung von Bedarfsträgerforderungen für Cyber/ IT, IT-Architektur-/ IT-Service Management sowie konzeptionelle Weiterentwicklung der Aus-, Fort- und Weiterbildung von IT-Personal,
- Digitale Verwaltung, d.h.
  Informationsmanagement, Open Government sowie Koordination von Anfragen für Cyber/ IT nach dem Informationsfreiheitsgesetz (IFG),
- Geoinformationswesen der Bundeswehr, d.h.
  Koordinierung der GeoInfo-Unterstützung für das IT-System der Bundeswehr (IT-SysBw), Europäisierung des Geoinformationswesens sowie Verantwortung für den Leistungsprozess „Geoinformationswesen sicherstellen“.

Die Unterabteilung CIT II[11] nimmt mit fünf Referaten im Schwerpunkt Aufgaben für Realisierung (BUILD) sowie für operativen Betrieb und Schutz (RUN) von IT-Services wahr, wobei die Rolle der bzw. des CISO Ressort bei der Unterabteilungsleiterin bzw. dem Unterabteilungsleiter CIT II liegt. Die Aufgaben umfassen die Bereiche:

- Einsatz und Betrieb des IT-Systems der Bundeswehr (IT-SysBw), d.h.
  Grundsatzangelegenheiten und Steuerung des IT-SysBw, Lage IT-SysBw, Verantwortung für

[10] Verortung innerhalb der Abteilung CIT ist im Zuge der Feinausplanung zu prüfen.
[11] Verortung IT-Betrieb BMVg (IUD III 3) wird bis zum Ende des vierten Quartals entschieden.

den Leistungsprozess „Führungsunterstützung sicherstellen“ (zukünftig IT-Servicebereitstellung sicherstellen), Bedarfskoordinierung der IT-Serviceprovider/ BWI sowie die IT-Koordinierung BMVg/ Bw

- Schutz des IT-SysBw, d.h.
  Umsetzung der sicheren IT-Architektur, Cyber-Abwehr, Informationssicherheit, Krypto-Sicherheit, Akkreditierung sowie IT-Krisenmanagement
- Core Services, d.h.
  Realisierung von Basis-, Querschnitts- und Infrastrukturdiensten im IT-SysBw sowie für die Vertragssteuerung der BWI
- Community of Interests (COI) und Communications (Comms) Services, d.h.
  Realisierung von Anwendungsdiensten für Einsatz und Übungen
- Standard-Anwendungs-Software-Produkt-Familien (SASPF), d.h.
  Realisierung von Anwendungsdiensten für Logistik und Administration durch SASPF und Systeme in Nutzung (SinN).

Neben der ministeriellen Steuerung der technologischen/ technischen Weiterentwicklung Cyber/ IT durch die neue Abteilung CIR verbleiben einsatzbezogene und rechtliche Verantwortlichkeiten in Bezug auf den CIR in den zuständigen Abteilungen Strategie und Einsatz sowie Recht. Diese Aufgaben gilt es im Zuge der weiteren Ausplanung unter Berücksichtigung der Organisationsanalyse des BMVg zu prüfen.

Für die Abteilung CIT ergibt sich ein anfänglicher Bedarf von ca. 130 Dienstposten, von denen voraussichtlich 95 Dienstposten mit ihren Aufgaben von anderen Referaten übertragen werden können.

Darüber hinaus besteht ein geringer Mehrbedarf, welcher der Stärkung Cyber/ IT relevanter Aufgaben, insbesondere in den Bereichen Stellung des Ressort-CIO, Informationssicherheit, Innovationsmanagement, GeoInfoWBw sowie unternehmerische Steuerung der BWI als Inhouse-Gesellschaft dient. Die Dotierung dieses zusätzlichen Dienstpostenbedarfs für das Spitzenpersonal umfasst:

- 1 DP B9
- 1 DP B6
- 3 DP A16/ B3

Im Rahmen der Bündelung der Cyber/ IT relevanten Aufgaben in der neuen Abteilung CIT wird eine Verlegung von voraussichtlich 6 Dienstposten von Bonn nach Berlin erforderlich. Hinsichtlich des aufgezeigten Mehrbedarfs entfällt die Mehrheit auf den Standort Berlin und 2 Dienstposten auf den Standort Bonn.

5.2 Militärischer Organisationsbereich Cyber- und Informationsraum

Auf Basis der Auflagen, Ableitungen und Erfolgsfaktoren ist ein neuer militärischer Organisationsbereich CIR konzipiert worden, der sich durch folgende Mehrwerte auszeichnet:

- Die zukünftige Inspekteurin bzw. der zukünftige Inspekteur CIR nimmt die Verantwortung für die Dimension CIR für die Bundeswehr zentral wahr.
- Ein ebenengerechter, durchsetzungsfähiger und eindeutiger PoC ist national und international etabliert.
- Das Leistungsvermögen der Bundeswehr im CIR wird durch eine angemessene Abbildung der Relevanz der Dimension gestärkt.
- Der Schutz eigener Netze wird zukünftig als Dauereinsatzaufgabe abgebildet.
- Die Bedarfsträgerforderungen für die Themenfelder 2 (Potenziale mobilisieren) und 5 (Karrierepfade) der Agenda Attraktivität für den Bereich CIR werden prominent in die Hand einer eigenen Inspekteurin bzw. eines eigenen Inspekteurs gegeben.
- Die Handlungsmöglichkeiten einer eigenständigen Organisationshoheit werden agiler.
- Die Zukunfts- und Weiterentwicklung wird CIR-gemeinsam harmonisiert.

Diese Mehrwerte werden durch die nachfolgende organisatorische Ausgestaltung des Organisationsbereichs CIR erzielt. Dafür wird ein schrittweises evolutionäres Vorgehen empfohlen.

Eine Startaufstellung zur Übernahme der truppendienstlichen Führungsaufgaben und zur Schaffung erster fachlicher Mehrwerte im Organisationsbereich CIR ist für 2017 vorgesehen.

In 2017 werden vorhandene Organisationselemente mit einem Dienstpostenumfang von ca. 13.700 Dienstposten zusammengeführt. Die Wanderungsbilanz setzt sich zusammen aus:

- FüUstgKdoBw, KdoStratAufkl, ZOpKomBw inkl. der jeweiligen unterstellten Dienststellen,
- Anteile BAAINBw und IT-ZentrumBw.

Darüber hinaus wurde ein Bedarf von 290 Dienstposten für die Startaufstellung in 2017 identifiziert:

- Grundbefähigung truppendienstliche Führung des Organisationsbereiches CIR (230[12] DP)
- Fachlicher Mehrwert für Zentrum Cyber-SicherheitBw (40 DP)
- Fachlicher Mehrwert Zentrum Cyber-Operationen (20 DP).

Hierfür wird ein Infrastrukturbedarf am Standort Bonn für maximal 230 Dienstposten entstehen. Dieser wird sich in Abhängigkeit der konkreten Alimentierung durch das Kommando Streitkräftebasis

[12] Ohne Berücksichtigung Alimentierung durch SKB und ggf. andere Organisationsbereiche.

entsprechend reduzieren. Darüber hinaus entsteht ein geringer Infrastrukturbedarf für 40 Dienstposten in Euskirchen und 20 Dienstposten in Rheinbach.

Alle bisherigen Standorte der in den Organisationsbereich CIR zu überführenden Dienststellen bleiben erhalten. Ebenso bleiben alle bisherigen B6+ Dienstposten an den derzeitigen Standorten.

Für die Startaufstellung Organisationsbereich CIR ist für 2017 folgende Organisation umzusetzen:

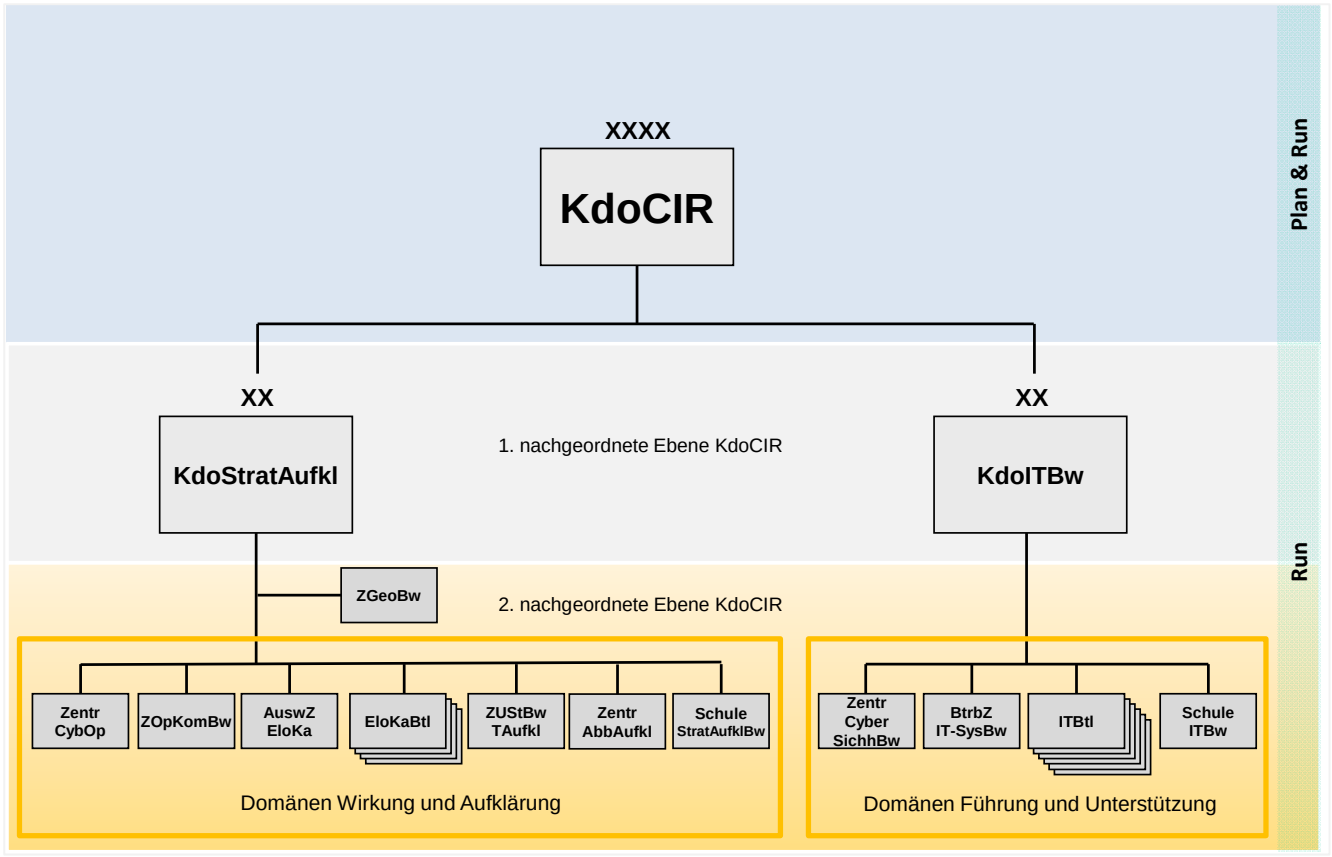

Abbildung 5: Startaufstellung Organisationsbereich Cyber- und Informationsraum 2017

Kommando Cyber- und Informationsraum

Die truppendienstliche und fachliche Führung des neuen Organisationsbereiches CIR ist Aufgabe des KdoCIR. Der Stab des KdoCIR umfasst – neben der Kommandoführung und einem Stabsquartier – drei Abteilungen.

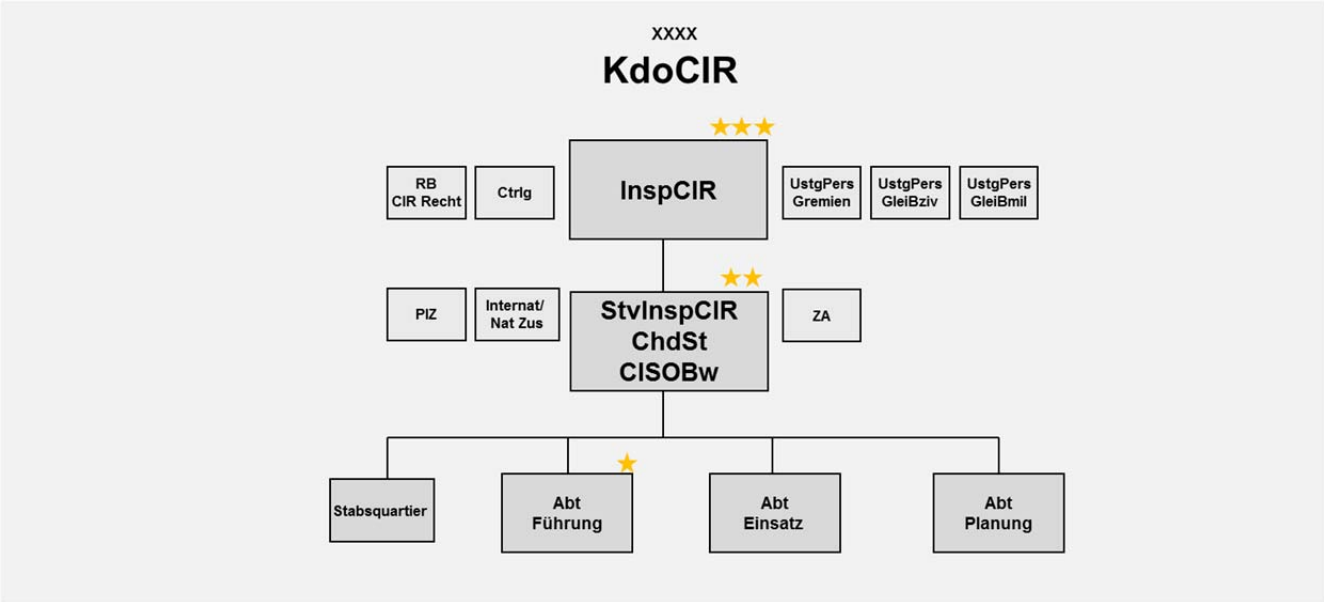

Abbildung 6: Startaufstellung KdoCIR 2017

Für die Startaufstellung 2017 ist im Kommandostab zunächst mit ca. 230 Dienstposten eine erste Arbeitsfähigkeit gegeben. Das KdoCIR ist in Bonn, Hardthöhe stationiert.

Für die Startaufstellung besteht nachfolgender Bedarf an Spitzendienstposten:

- 1 DP B9
- 1 DP B7
- 1 DP B6

Der Bereich der Kommandoführung umfasst die Inspekteurin oder den Inspekteur und die Stellvertreterin bzw. den Stellvertreter des bzw. der Insp (StvInsp) (zunächst in Personalunion Chef des Stabes) inklusive der entsprechenden Adjutanturen und Vorzimmer. Für die Umsetzung der Vorgaben der bzw. des CISO Ressort zur Informationssicherheit in der Bundeswehr wird die Rolle der oder des Chief Information Security Officer der Bundeswehr (CISOBw) eingerichtet und der oder dem StvInspCIR übertragen. Der CISOBw trägt die operationelle Durchführungsverantwortung für die Informationssicherheit in der Bundeswehr gemäß den Leitlinien des oder der Ressort-CIO.

Des Weiteren sind in der Kommandoführung das Referat Zentrale Angelegenheiten, das Referat Controlling, die Presse- und Informationszentrale sowie das Personal für Beteiligungsgremien und Interessenvertretungen ausgeplant. Erste fachliche Mehrwerte für den Organisationsbereich CIR werden

durch ein Referat für die Steuerung und Koordinierung der nationalen und internationalen Zusammenarbeit sowie ein Referat zur rechtlichen Beratung für CIR-spezifische Themen erzeugt.

Die Abteilung Führung unterstützt die Inspekteurin bzw. den Inspekteur in der truppendienstlichen Führung, d.h. in Personalfragen, in Fragen der militärischen Sicherheit, der Verwaltung, der Logistik, der IT-Unterstützung/ IT-Sicherheit der Dienststelle sowie in sanitätsdienstlichen Fragen.

Die Abteilung Einsatz wird in 2017 nur eine rudimentäre Grundbefähigung besitzen. Diese beinhaltet jedoch bereits die aus dem BAAINBw zu überführenden Aufgaben und Personal zur Unterstützung der oder des StvInspCIR bei der Wahrnehmung ihrer bzw. seiner Aufgaben als CISOBw.

Die Abteilung Planung wird in 2017 mit Schwerpunkt Fähigkeiten zur weiteren organisatorischen Ausplanung des Organisationsbereiches CIR besitzen.

Für die geplante Entwicklung der Struktur des KdoCIR ab 2018 sind zwei Punkte besonders hervorzuheben:

- Stärkung der Inspekteurin bzw. des Inspekteur CIR in ihrer bzw. seiner richtungsgebenden Funktion durch Zusammenführung der zuständigen Elemente für die Weiterentwicklung und Ausbildung des gesamten Kommandobereichs CIR in der Abteilung Planung.
- Stärkung des operationellen Beitrages in der Abteilung Einsatz durch Aufbau eines gemeinsamen Lagezentrums und eines multinationalen Führungselementes, welches auch ein Führungselement für den Einsatz bereitstellen kann.

Erste nachgeordnete Ebene Kommando Cyber- und Informationsraum

Kommando Strategische Aufklärung (KdoStratAufkl)[13]

Für die Startaufstellung in 2017 wird das Kommando Strategische Aufklärung (KdoStratAufkl) mit seinem nachgeordneten Bereich in den Organisationsbereich CIR überführt. Zusätzlich wird dem KdoStratAufkl das Zentrum Operative Kommunikation der Bundeswehr (ZOpKomBw) unterstellt.

Das KdoStratAufkl konzentriert sich auf das Nachrichtenmanagement, die Aufklärung und die Wirkung im CIR. Es erstellt eine Nachrichtenlage, die sich auf die taktische und operative Ebene konzentriert und den aktuellen Risiken und hybriden Bedrohungen gerecht wird. Gleichzeitig ist diese Lage den Entscheidungsträgern und Führungsgehilfen aller Ebenen zur Verfügung zu stellen. Darüber hinaus operiert das Kommando im Auftrag mit seinen Fähigkeiten im CIR.

Für die geplante Entwicklung der Struktur des KdoStratAufkl ab 2018 ist besonders hervorzuheben, dass das KdoStratAufkl von seinen bisherigen fachlichen Aufgaben in der Weiterentwicklung der streitkräftegemeinsamen Ausbildung im Bereich des Militärischen Nachrichtenwesens (MilNW), der Weiterentwicklung der Fähigkeiten im KdoStratAufkl und der Koordination der übergreifenden streit-

[13] Ein Kommando für Aufklärung und Wirkung.

kräftegemeinsamen Fähigkeiten im MilNW nach Schaffung der Voraussetzungen im KdoCIR entbunden wird. Die Abteilung Weiterentwicklung wird in Gänze an die Abteilung Planung des KdoCIR abgegeben, um so eine Planung aus der ganzheitlichen Perspektive des Cyber- und Informationsraums zu etablieren.

Der Stationierungsort des KdoStratAufkl ist unverändert Grafschaft-Gelsdorf/ Bad Neuenahr.

Führungsunterstützungskommando der Bundeswehr (FüUstgKdoBw)
Für die Startaufstellung in 2017 wird das Führungsunterstützungskommando der Bundeswehr (FüUstgKdoBw) mit seinem nachgeordneten Bereich in den Organisationsbereich CIR überführt. Zusätzlich wird dem FüUstgKdoBw das Zentrum für Informationstechnik der Bundeswehr (IT-ZentrumBw) unterstellt.

Als unterstützender Schritt zu einem besseren gemeinsamen Verständnis nach innen und außen wird das Führungsunterstützungskommando der Bundeswehr bereits in der Startaufstellung 2017 in „Kommando Informationstechnik der Bundeswehr (KdoITBw)“ umbenannt. Aufgrund einer attraktiveren Wahrnehmung durch eine zivil vergleichbare Bezeichnung kann insbesondere die Nachwuchsgewinnung von dieser Maßnahme profitieren. Eine vergleichbare Umbenennung erfolgt im nachgeordneten Bereich.

Das KdoITBw verantwortet neben der truppendienstlichen Führung des unterstellten Bereiches den Einsatz und Betrieb des IT-SysBw, sowohl mit Blick auf interne als auch externe IT-Serviceprovider. Diese zentrale Bedarfskoordinierung der IT-Leistungserbringung wird in einer neuen Abteilung Supply Management wahrgenommen. Die Beratung von Verantwortungsträgern/ Entscheidern, der Abruf von Leistungen, Leistungsänderungen und die Priorisierung der Leistungsabrufe erfolgt über alle IT-Serviceprovider, einschließlich BWI, gleichfalls aus dieser Abteilung.

Für die geplante Entwicklung der Struktur des KdoITBw ab 2018 ist besonders hervorzuheben, dass das KdoITBw von seinen bisherigen fachlichen Aufgaben für die IT-Ausbildung sowie die operationelle Weiterentwicklung des IT-SysBw MilNW nach Schaffung der Voraussetzungen im KdoCIR entbunden wird. Die Abteilungen Weiterentwicklung und Ausbildung werden in Gänze an die Abteilung Planung des KdoCIR abgegeben, um auch hier eine Planung aus der ganzheitlichen Perspektive des Cyber- und Informationsraums zu gewährleisten.

Der Stationierungsort des KdoITBw ist unverändert Bonn, Hardthöhe.

Zweite nachgeordnete Ebene Kommando Cyber- und Informationsraum

Elemente, die derzeit dem KdoStratAufkl sowie dem FüUstgKdoBw unterstellt sind sowie das Zentrum Operative Kommunikation werden in den Organisationsbereich CIR übernommen und setzen dort ihren originären Auftrag an den derzeitigen Standorten fort. In einigen dieser Elemente werden

bereits in 2017 erste fachliche Mehrwerte durch Binnenoptimierung bzw. moderaten Personalaufwuchs erzeugt.

Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw)

In der Startaufstellung 2017 ist das Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw) zur Aufstellung des Organisationsbereiches CIR in Gänze zu überführen. Um den Veränderungsbedarf zu Beginn so gering wie möglich zu halten und das KdoCIR in der initialen Startaufstellung nicht zusätzlich zu belasten, bleibt das ZGeoBw zunächst unverändert dem KdoStratAufkl truppendienstlich unterstellt.

Der Stationierungsort des ZGeoBw ist unverändert Euskirchen mit den bereits heute bestehenden Außenstellen.

Für 2018 sollte zur Sicherstellung der Weiterentwicklung und Zukunftsfähigkeit der GeoInfo-Unterstützung eine unmittelbare truppendienstliche Unterstellung des ZGeoBw unter das KdoCIR untersucht werden, um so insbesondere die Bildung eines "Europäischen Zentrums für Geoinformationen" zu fördern und Schnittstellen ohne fachlichen Mehrwert zu minimieren.

Zentrum für Informationstechnik der Bundeswehr (IT-ZentrumBw)

Das Zentrum für Informationstechnik der Bundeswehr (IT-ZentrumBw) ist bereits 2017 in Gänze aus dem Geschäftsbereich des BAAINBw herauszulösen, dem KdoITBw zu unterstellen und in ein Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) umzugliedern. Die weitere Wahrnehmung der bisherigen Aufgaben für IT-Sicherheit und Unterstützungsleistungen für Projekte im Auftrag des BAAINBw ist dabei sicherzustellen.

Für die geplante Entwicklung ab 2018 ist besonders hervorzuheben, dass die Teile des früheren IT-ZentrumBw, die zunächst auch aus dem neuen ZCSBw heraus Projektaufgaben für das BAAINBw durchführen, ausgegliedert werden und ein neues Zentrum Softwarekompetenz IT-System Bundeswehr bilden.

Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw)

In der Startaufstellung 2017 wird das heutige IT-ZentrumBw in „Zentrum für Cyber-Sicherheit der Bundeswehr“ umbenannt und dem KdoITBw unterstellt. Eingegliedert wird die bisher im BAAINBw verortete IT-Sicherheitsberatungs- und Akkreditierungsstelle. Die heute verteilten operativen Aufgaben, Zuständigkeiten und Verantwortlichkeiten der IT-/ Cyber-Sicherheit werden damit weitestgehend zusammengeführt. Zur Stärkung vorhandener fachlicher Fähigkeiten sind für das ZCSBw 40 zusätzliche Dienstposten bereits in 2017 vorgesehen. Die Stärkung erfolgt bei den Fähigkeiten zum Schutz des IT-Systems der Bundeswehr, einschließlich einer 24/7-Befähigung, zur Verbesserung des Cyber-Sicherheitslagebildes und zur Steigerung der Befähigung zur ressortübergreifenden Zusammenarbeit.

Der Hauptstationierungsort des ZCSBw ist Euskirchen.

Ab 2018 wird das ZCSBw zum zentralen Element für die Gewährleistung der Informationssicherheit insbesondere im Hinblick auf den Schutz des IT-Systems der Bundeswehr gegen Angriffe aus dem Cyber-Raum ausgebaut. Dazu werden die fachfremden Anteile für das neue Zentrum Softwarekompetenz IT-System Bundeswehr ausgegliedert und gleichzeitig die vorhandenen Fähigkeiten für Cyber-Abwehr gestärkt sowie weiterentwickelt. Die entsprechenden Elemente der BWI werden mit dem ZCSBw eng verzahnt. Für eine höhere fachliche Professionalisierung in den Einsätzen, stellt das ZCSBw zukünftig Cyber-Sicherheitspersonal für Einsatzkontingente als Security Operation Center im Einsatz bereit.

Für diesen Aufbau zukunftsorientierter Cyber-Abwehrfähigkeiten sind zusätzliche Dienstposten erforderlich. Diese werden u.a. für Fähigkeiten zur Cyber-Sicherheit von Waffensystemen, zur Sensibilisierung der Mitarbeiterinnen und der Mitarbeiter, zur nationalen und internationalen Zusammenarbeit, zur Durchführung von Schwachstellenanalysen und Penetrationstests eigener Systeme sowie zur querschnittlichen fachlichen Unterstützung der Einsätze und Dienststellen der Bundeswehr benötigt.

Die Weiterentwicklung der IT-Sicherheits- und Kryptoorganisation der Bundeswehr erfolgt im Inland durch Einrichtung von vier dem ZCSBw unmittelbar unterstellten Regionalzentren und einer noch festzulegenden Anzahl von regionalen Außenstellen zur adäquaten fachlichen Unterstützung der Organisationsbereiche und Dienststellen der Bundeswehr. Dies erfordert u.a. einen Transfer von Aufgaben und Dienstposten der IT-Sicherheits- und Kryptoorganisation der Bundeswehr aus den Organisationsbereichen und Dienststellen an den Organisationsbereich CIR[14].

Zentrum Cyber-Operationen (ZCO)

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[15] unterstellt. Mit einem Aufwuchs von 20 Dienstposten bereits in 2017 werden insbesondere Fähigkeiten zur Aufklärung und zum Red-Teaming ausgebaut, um bessere Beiträge zu einer gemeinsamen Cyber-Lage und zum Schutz eigener Netze und Waffensysteme leisten zu können.

Ziele der weiteren Entwicklung ab 2018 sind 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 sowie der Elemente zur wirkungsvollen Unterstützung des ZCSBw und der Truppe im Rahmen von Übungen (Red Teams). Für diesen weiteren Ausbau vorhandener sowie den Aufbau zusätzlich erforderlicher, zeitgemäßer Fähigkeiten zur Durchführung von Cyber-Operationen werden zusätzliche Dienstposten benötigt.

[14] Der detaillierte Umfang ist im Zuge der Feinausplanung zu prüfen.
[15] Derzeit ist die Gruppe CNO Teil der Abteilung Einsatz im KdoStratAufkl.

Zukünftige Mehrwerte und Fähigkeitsaufwuchs

Ab 2018 sind die Fähigkeiten des Organisationsbereich CIR durch Umsetzung der identifizierten fachlichen Mehrwerte weiter zu stärken. Diesen Bedarf gilt es in den kommenden Jahren durch das KdoCIR weiter zu untersuchen und zu priorisieren.

Abbildung 7: Identifizierte fachliche Mehrwerte ab 2018

Bereits in der Startaufstellung werden das Zentrum Cyber-Sicherheit der Bundeswehr und das Zentrum Cyber-Operationen mit ersten Dienstposten gestärkt. Der zuvor beschriebene Fähigkeitsaufwuchs für diese Elemente sollte auch ab 2018 weiter priorisiert erfolgen.

Zentrum Softwarekompetenz IT-System der Bundeswehr (ZSKBw)

Das ZSKBw wird erst nach der Startaufstellung durch Ausgliederung aus dem Zentrum Cyber-Sicherheit der Bundeswehr unter Personalaufwuchs aufgestellt werden. Dieses neue Zentrum sollte eine Kapazität zur Erfüllung von Softwareforderungen sowohl autark als auch in abgestuften Formen von der Forderungsanalyse über das Prototyping bis hin zur Eigenprogrammierung erhalten. Die Einbindung innovativer Ideen soll über ein Verbindungselement ermöglicht werden, dass einerseits die Expertise im Zentrum aktuell hält und andererseits in der Lage ist, neue Entwicklungen auf Anwendungspotenzial in der Bundeswehr zu bewerten. Die bisher im IT-ZentrumBw wahrgenommenen Unterstützungsleistungen für Projekte im Auftrag des BAAINBw werden auch weiterhin über geeignete Service Level Agreements sichergestellt. Darüber hinaus können Aufgaben im Rahmen der Beratung von Projektleiterinnen und Projektleitern sowie der betrieblichen Integration von IT-Services in das IT-System Bw wahrgenommen werden.

Ausbau Stab KdoCIR

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 Command-Element zu leisten, wird durch den Aufwuchs der Abteilung Einsatz im Stab KdoCIR erreicht.

Gemeinsames Lagezentrum

In einem Gemeinsamen Lagezentrum des Stabes im KdoCIR soll zukünftig ein fusioniertes Lagebild CIR erarbeitet und bundeswehrweit sowie ressortübergreifend zur ebenengerechten Information zur Verfügung gestellt werden. Innerhalb der Bundeswehr sind dazu die Militärische Nachrichtenlage, die Lage im Informationsumfeld, die Weltraumlage, die Zivile Lage, die Lage C-IED, die Betriebslage IT-SysBw und die Cyber-Sicherheitslage auf Grundlage eines Recognized Environmental Picture zu einem höheren Erkenntnisgrad zu verknüpfen. Die Eigene Lage anderer Organisationsbereiche wird nicht eingebunden, da sie nicht in die Verantwortung des Organisationsbereiches CIR fällt.

Zentrum Nachrichtenlage

Mit einem zukünftigen Zentrum Nachrichtenlage soll das Militärische Nachrichtenwesen eine umfassende Nachrichtenlage zur Verfügung stellen, um den gestiegenen Anforderungen gerecht zu werden. Dies dient im Schwerpunkt der Unterstützung des Einsatzes in allen seinen Phasen und der Krisenvorsorge. Hierzu sind auch moderne Möglichkeiten, wie z.B. des Operations Research sowie der Simulation und Modellbildung zu nutzen.

Zentrum für Geoinformationswesen der Bundeswehr

Das Zentrum für Geoinformationswesen der Bundeswehr soll einen verbesserten Beitrag zur Analyse und Durchdringung der Dimension CIR sowie für das CIR-Lagebild leisten. Dazu sind im Schwerpunkt Fähigkeiten in den Bereichen Geoinformationssysteme, Big Data Geo-Analyse, lagebezogene Landeskundliche Beratung und alternative Verfahren zur Navigation, Positionierung und Zeitfestlegung zu stärken.

6. Ergänzende Handlungsempfehlungen

Zur Begleitung der vorgestellten organisatorischen Empfehlungen ist es erforderlich, weitere Maßnahmen einzuleiten, um die Ziele, die mit den Änderungen erreicht werden sollen, wirkungsvoll zu unterstützen. Dazu wurden mit der Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg die Neuordnung von Verantwortlichkeiten, Kompetenzen und Aufgaben angewiesen – aber auch weitere Untersuchungen beauftragt, beispielsweise zum Thema Expertise-Aufbau.

Nachfolgende Maßnahmen flankieren die organisatorischen Maßnahmen und zielen darauf ab, die neuen Strukturen nachhaltig mit geeignetem Personal zu besetzen. Darüber hinaus werden einige Maßnahmen aufgezeigt, die als „Quick Hits“ bereits in der Umsetzung sind und auch kurzfristig sichtbare Ergebnisse liefern werden.

6.1 Maßnahmen im Bereich Personal

Die ergänzenden Maßnahmen im Bereich Personal sind in einem Verständnis geschrieben, Zielvorgaben in den Handlungsfeldern der Personalstrategie der Bundeswehr für den Bereich „Cyber/ IT“ zu spezifizieren und mit ersten inhaltlichen Impulsen zu Karrierewegen, neuen Instrumenten der Personalgewinnung oder Bildungs- und Qualifizierungsmaßnahmen zu bereichern.

Entwicklung von Karrierewegen

Unter Berücksichtigung der hohen Dynamik im IT-Sektor und der fortschreitenden Digitalisierung ist davon auszugehen, dass sich bestehende Berufsbilder weiterhin schnell wandeln werden. Dies betrifft insbesondere das Personal im Organisationsbereich CIR, aber mittelbar auch die rund 20.000 Bundeswehr-Mitarbeiter und Mitarbeiterinnen, die bereits heute auf IT-nahen Dienstposten arbeiten. Für das Personal im Aufgabenbereich CIR[16] sind daher anpassungsfähige und dynamische Werdegangsmodelle vorzusehen, bei dem der Personalbedarf zeitnah auf die tatsächlich benötigten Fähigkeiten und Fertigkeiten ausgerichtet werden kann und das gleichzeitig einen kontinuierlichen Kompetenzzuwachs sicherstellt.

Aus diesem Grund wird empfohlen, bereits begleitend zur Phase der Aufstellung des Organisationsbereiches CIR bundeswehrgemeinsame Karrierewege und Werdegänge zu konzipieren, die dieser hohen Dynamik Rechnung tragen und zugleich als Attraktivitätsmotor für den Arbeitgeber Bundeswehr im Wettbewerb mit Dritten um Talente wirken.

[16] Neben den bereits bekannten Personalkategorien aus den Bereichen MilNW, OpKomBw und GeoInfoDBw gehört dem Organisationsbereich CIR auch IT-Personal an. Unter IT-Personal werden diejenigen militärischen und zivilen IT-Fach- und Führungskräfte der Bundeswehr verstanden, die Aufgaben in den Bereichen Weiterentwicklung, Realisierung, Einsatz und Betrieb sowie Schutz des IT-SysBw wahrnehmen (z.B. F&T-Verantwortliche im Bereich Informationstechnologie, IT-Projektleiter, IT-Verantwortliche, IT-Koordinatoren, IT-Administratoren, IT-Nutzerbetreuer, IT-Ausbilder und IT-Sicherheitspersonal). Davon abzugrenzen sind IT-Anwender/-Bediener, die zur Wahrnehmung ihrer jeweiligen Aufgaben lediglich die zur Verfügung gestellte IT-Ausstattung benutzen.

Die Personalstrategie der zukünftigen Inhouse-Gesellschaft BWI bietet bei der Entwicklung von solchen Modellen einen hilfreichen Orientierungsrahmen und eröffnet zudem Chancen für die ganzheitliche Betrachtung eines gemeinsam gedachten Cyber/ IT-Personalkörpers[17]. Langfristiges Ziel sollte es sein, einschlägige Fachkarrieren und Fachlaufbahnen zu entwickeln, die auch ressortübergreifend (z.B. über vergleichbare Anforderungsprofile) anerkannt sind und auf die fachliche Tätigkeit und Spezialisierung des Personals zu fokussieren. Bei dieser ganzheitlichen Betrachtung ist auch die Rüstungslaufbahn der Fachrichtung Informationstechnik und Elektronik (ITE) einzubeziehen.

In einem ersten Schritt ist zunächst die Formulierung einer Verwendungsaufbaukonzeption für das Cyber/ IT-Personal vorzusehen, die grundlegende fachliche Forderungen und eine umfassende Bedarfsträgerforderung an die Personalführung für die Gestaltung individueller Personalentwicklungsmaßnahmen beinhaltet.

Innovative Wege der Personalgewinnung

Die fachlichen Zuständigkeiten des Organisationsbereiches Personal anerkennend wird seitens des Aufbaustabs CIR empfohlen, die bestehenden Personalgewinnungsmaßnahmen um neue, flexible und innovative Personalgewinnungsinstrumente zu ergänzen. Ziel ist es hierbei, neue oder bislang unterrepräsentierte Bewerbergruppen für noch zu spezifizierende Fachaufgaben im neuen Organisationsbereich CIR in einem hoch wettbewerblichen Arbeitsmarkt erschließen zu können, die bisher aufgrund anderer dominierender Faktoren nicht in Betracht gezogen wurden (z.B. wegen fehlender Eignung als Soldatin oder Soldat oder wegen explizit fehlendem Interesse an einer Tätigkeit als Soldatin oder Soldat, Menschen mit Migrationshintergrund, Staatsangehörige anderer Länder). Zu möglichen neuen Zielgruppen zählen auch Kandidatinnen und Kandidaten ohne formalen Bildungsabschluss (z.B. Studienabbrecherinnen und Studienabbrecher) oder Bewerberinnen und Bewerber aus fachfremden Disziplinen, die über geeignete informell oder nicht-formell erworbene Kompetenzen verfügen und eine hohe Motivation für eine Auseinandersetzung mit Cyber-Aufgabenfeldern mitbringen, aber keine klassische MINT[18]-Vorbildung nachweisen können[19].

Die Durchführung von IT-Turnieren als mögliches Instrument der Personalrekrutierung (z.B. in Form von LAN-Partys für die Rekrutierung von Talenten aus der Gamer-/ E-Sport-Szene) ist genauso in Betracht zu ziehen wie aktiv beworbene Stipendienmöglichkeiten (Cyber-Stipendien), die eher die rein an den Fachaufgaben interessierten Gruppen (z.B. „Nerds“ für Aufgaben der Cyber-Abwehr bzw. der Informationssicherheit) ansprechen. Die Grenzen dieser Verfahren sind jedoch noch näher durch die fachlich zuständigen Stellen zu untersuchen.

[17] Bspw. durch gemeinsame Aus-, Fort- und Weiterbildungen, gegenseitigen Personalaustausch, Rotationsmöglichkeiten.
[18] MINT steht für die Fächergruppen Mathematik, Ingenieurwissenschaften, Naturwissenschaften und Technik.
[19] Beamtenrechtliche und auch tarifrechtliche Vorgaben sowie weitere rechtliche Grenzen sind zu berücksichtigen.

Gleiches gilt für die Aussprache von Cyber-Stipendien. Auch hier sind noch vertiefende Untersuchungen in Abhängigkeit der Ausgestaltung des Studiums an den Universitäten der Bundeswehr sowie der Auswahl und des künftigen Bedarfs an Cyber-Personal durchzuführen. Mithilfe von Cyber-Stipendien (in Anlehnung an die bestehende Studienförderung) können angeworbene Interessentinnen und Interessenten analog zu den studierenden Offizieranwärterinnen und -anwärtern an den Universitäten der Bundeswehr (UniBw) wissenschaftlich ausgebildet und dann zunächst als Tarifbeschäftigte beschäftigt oder bereits – bei Vorliegen der notwendigen Qualifikationen – unmittelbar als Tarifbeschäftigte eingestellt werden.

Schließlich ist auch der Binnenarbeitsmarkt der Bundeswehr auf die Gewinnung von Fachpersonal im Aufgabenbereich CIR auszurichten. Dazu sind einschlägige informelle, nicht-formelle und formell erworbene Fähigkeiten, Fertigkeiten und Kompetenzen von Bundeswehrangehörigen anerkennungsfähig zu erfassen und im Rahmen von Bewerbungsverfahren für mögliche Stellenbesetzungen zu berücksichtigen.

Aus-, Fort- und Weiterbildung (als Teil der Personalentwicklung)

Die Fachaufsicht über das berufsqualifizierende Aus-, Fort- und Weiterbildungsangebot des Organisationsbereich CIR wird der Abteilung Planung im KdoCIR[20] obliegen. Eine der wesentlichen Aufgaben dieser Abteilung wird es sein, die Angebote der Ausbildungseinrichtungen und Schulen langfristig auf die organisationsbereichsspezifische Formulierung konkreter Aus-, Fort- und Weiterbildungsziele und eindeutiger Kompetenzprofile auszurichten. Von Beginn an ist für einschlägiges Fachpersonal (insbesondere nichtstudierte Soldateninnen und Soldaten) an der IT-Schule der Bundeswehr ein bedarfsgerechtes, modulares und kontinuierliches Bildungsangebot für Fähigkeiten im Bereich CIR aufzulegen, welches einerseits inhaltlich fokussiert und andererseits den zeitlich gestrafften Kompetenzerwerb steuert. Zugleich sollte die Ausbildungssystematik den weiteren Verwendungsaufbau von Fachkräften sowie von Expertinnen und Experten konsequent unterstützen. Für den Cyber-Bereich sind dabei neben den bereits bestehenden auch gänzlich neue Aus-, Fort- und Weiterbildungslehrgänge zu entwickeln, die sowohl Grundkurse zu Cyber- und Netzverteidigung enthalten, aber auch Kenntnisse in IT-Management vermitteln sowie zu umfänglichen Programmierkenntnissen führen.

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. Die Universität der Bundeswehr München wird dabei zu der zentralen, wissenschaftlichen Aus-, Fort- und Weiterbildungsstätte der Bundeswehr für Tätigkeiten im Bereich der Cyber-Verteidigung und Cyber-Sicherheit ausgebaut. Mithilfe der Einrichtung neuer einschlägiger Studiengänge, wie etwa den

[20] Für den GeoInfoDBw liegt die Verantwortung bei der Leiterin bzw. dem Leiter des Geoinformationsdienstes der Bundeswehr.

Master-Studiengang Cyber-Sicherheit, erhalten Angehörige der Bundeswehr eine qualifizierte wissenschaftliche Ausbildung. Die Ausbildungskapazitäten sind international auszurichten und auch anderen interessierten Sicherheitsbehörden, Ressorts (u.a. Geschäftsbereich des Bundesministeriums des Innern) und Bündnispartnern als Hochwertbeitrag der Bundeswehr für die gemeinsame Aufgabe in der gesamtstaatlichen Sicherheitsvorsorge anzubieten. Für Spezialistinnen und Spezialisten aus nicht-technischen Bereichen (z.B. der Operativen Kommunikation) sowie der Cyber-Reserve werden an der Universität der Bundeswehr München zudem Fort- und Weiterbildungsmöglichkeiten in einschlägigen Cyber-Fachgebieten angeboten.

Personalbindung und -führung

Um eine individuelle Betreuung und Entwicklung des Personals aus dem Organisationsbereich CIR zu ermöglichen, wird vorgeschlagen, eine auf den Organisationsbereich CIR abgestimmte Personalführungskomponente beim zuständigen Bundesamt für das Personalmanagement der Bundeswehr einzurichten. Diese sollte einen bedarfsgerechten[21], flexiblen und individuellen Personalservice ermöglichen und zugleich als zentrale Ansprechstelle der bzw. des InspCIR fungieren. Dazu ist noch zu untersuchen, ob die derzeit festgelegten Kompetenzbereiche oder andere personelle Ordnungsmittel grundlegend geändert bzw. durch Neugestaltungen erweitert werden.

Die Bundeswehr kann ihre Talente nicht primär über monetäre Anreize gewinnen oder halten, sondern über die Sinnhaftigkeit ihres Auftrags. Dennoch sollten die vorhandenen monetären Instrumente für den Talenterhalt und die Personalbindung (z.B. Zulagenmodelle für die Beschäftigten, höheres Eingangsamt, Sonderbesoldung, konkurrenzfähige Bezahlung) im Sinne einer verbesserten Arbeitgeberattraktivität konsequent auf ihre Anwendbarkeit auf den Personalkörper im Organisationsbereich CIR hin untersucht werden. Ergänzend hierzu ist ein organisationsbereichsinternes Portfolio nichtmonetärer Instrumente und Maßnahmen für die Personalbindung aufzulegen (z.B. neue Arbeits-/ Führungs-/ Teamstrukturen, Arbeitsplatzausstattung und Arbeitsplatzorganisation), das Rahmenbedingungen für die gewollte Innovationsfähigkeit des neuen Organisationsbereichs günstig beeinflusst.

[21] Darunter fallen auch flexible Beschäftigungsverhältnisse.

6.2 Entwicklung einer Identität des Organisationsbereiches

Die Identität und die Kultur des eigenständigen militärischen Organisationsbereiches CIR werden sich über längere Zeiträume bilden und prägen. Die Kultur erwächst innerhalb und aus dem Organisationbereich selbst heraus. In keinem Falle ist die Kultur durch eine Weisung „erlassbar“. Möglichweise wird die Natur der Kultur von CIR-Kräften eine andere sein als diejenige von Truppen, die ihr Selbstverständnis aus dem unmittelbaren Kampf und der Anwendung physischer Gewalt ziehen. Ob und inwiefern die einzelnen und langfristig gewachsenen Traditionslinien einzelner Truppengattungen sinn- und identitätsstiftend sein können, bleibt abzuwarten. Der eigenständige Organisationsbereich ist ein entscheidendes Merkmal für eine Abgrenzung im positiven Sinne. Diesem Organisationsbereich das Merkmal eines Uniformträgerbereiches oder anderer äußerer Kennzeichen zu zuschreiben ist sicherlich geeignet, einer Identitätsbildung noch kräftigeren Schub zu verleihen.

6.3 Quick Hits und ihre Mehrwerte

Das Erreichen von „Quick Hits“ dient dem Ziel im Wege des Veränderungsmanagements die Phase der weiteren Ausgestaltung des CIR durch sichtbare Erfolge und schnelle Resultate wirkungsvoll zu unterstützen.

Cyber-Cluster Universität der Bundeswehr München

Ein wesentlicher Pfeiler in der Personalstrategie der Bundeswehr ist immer die eigene Ausbildung von Personal gewesen. Mit der Einrichtung einer ressorteigenen Forschungseinrichtung an der Universität der Bundeswehr München wird die bundeswehreigene universitäre Forschung auch auf den Bereich Cyber-Verteidigung ausgeweitet. Ein internationaler Studiengang zur „Cyber-Sicherheit“ soll bereits 2018 beginnen und jährlich ca. 70 Absolventen hervorbringen.

Mit dessen institutioneller Anbindung an die wissenschaftliche Ausbildung ist somit auch eine Plattform für den Aufbau eines bundesweit einzigartigen Cyber-Clusters verbunden, der den Austausch und die Zusammenarbeit mit den (Sicherheits-)Behörden des Bundes und der Länder, den Ressorts, der Industrie, den Wissenschaftseinrichtungen und weiteren gesellschaftlichen Institutionen ermöglichen soll (z.B. über die Durchführung von Tagungen, Foren, Kooperationen, o.ä.). Mithilfe der zum Teil auch als Auftrags- und Ressortforschung angelegten wissenschaftlichen Arbeiten sollen zudem Produktentwicklungen aus Forschungsvorhaben unmittelbar angestoßen werden, die wertschöpfend bis hin zur Nutzung in der Bundeswehr (auch in Kooperation mit der Industrie) weiterentwickelt werden können.

Ein Cyber-Cluster Universität der Bundeswehr München unterstützt das Anliegen der Bundeswehr, eigene Forschungsziele durch den Aufbau einer aktuellen universitären Forschung zu „Cyber Defence“ auf internationalem Niveau effektiv verwirklichen zu können. Die Anbindung an die wissenschaftliche Ausbildung bietet zudem gute Chancen, ein sichtbares Zeichen für einen an der Fachauf-

gabe interessierten Personenkreis zu setzen. Damit wirkt das Cyber-Cluster mittelbar auch als Attraktivitätsinstrument für die Personalgewinnung.

Cyber-Reserve (Arbeitsbegriff)

Zur Erfüllung des Auftrags der Bundeswehr bei der gesamtstaatlichen Sicherheitsvorsorge wird eine hoch qualifizierte und einsatzfähige Cyber-Reserve aufgebaut, die dem Ziel dient, ein zusätzliches Kräfteelement im Inland zu bilden, welches der militärischen Führung und auch der politischen Leitung zur Abwehr von Cyber-Angriffen und zum Wirken im CIR zur Verfügung steht. Durch gemeinsames Üben und der übergreifenden Bündelung von Spezialistinnen und Spezialisten soll eine wirkungsvolle und State of the Art Cyber-Komponente aufgebaut werden. Ziel der Cyber-Reserve ist es schließlich, den Erfahrungsaustausch und den Wissenstransfer in einem Umfeld von rasanten technologischen Veränderungen mit vorhandenen Kräften, insbesondere unter Einbindung des an der Universität der Bundeswehr München angesiedelten Cyber-Clusters zu fördern.

Für die Cyber-Reserve sind vor allen Dingen die Fähigkeiten ausscheidender Berufs- und Zeitsoldaten gefragt, die bereits während ihrer aktiven Zeit für eine Rückkehr als aktive Reservistin bzw. aktiver Reservist zu gewinnen sind. Aber auch Freiwillige, Seiteneinsteigerinnen und Seiteneinsteiger sowie bislang Ungediente aus der gewerblichen IT-Wirtschaft, einschlägigen MINT-Berufen oder ähnlichen Professionen sind gefragt, die über Spezialisten-Ausbildungen oder herausragende Fähigkeiten, Fertigkeiten und Kompetenzen in einschlägigen IT-Bereichen bzw. IT-Funktionen verfügen. Für den Erfahrungsaustausch und den Wissenstransfer werden in einem einzurichtenden Circle of Excellence herausgehobene Spezialistinnen, Spezialisten und IT-Führungskräfte aus Wirtschaft, Verwaltung und Behörden zum Austausch in strategischen Handlungsfeldern benötigt.[22]

Mit dem Aufbau einer Cyber-Reserve werden die bisher ungenutzten Potenziale von hochqualifizierten Cyber-Spezialistinnen und Cyber-Spezialisten für die Aufgabenwahrnehmung bei der gesamtstaatlichen Sicherheitsvorsorge besser ausgeschöpft. Zugleich können die derzeit nicht oder nicht ausreichend vorhandenen, aber unverzichtbar benötigten Fähigkeiten und Kompetenzen für die Gewährleistung der Verfügbarkeit bundeswehreigenen informationstechnischen Systeme sowie der Begegnung übergreifender Cyber-Angriffe und Attacken gegen Staat, Wirtschaft und Gesellschaft besser abgerufen werden.

Cyber-Hygiene Check-Up

Bei Cyber-Angriffen werden im Schnitt immer noch über 200 Tage benötigt, um einen anspruchsvollen Angriffsvektor zu erkennen. Die Beseitigung dauert in der Regel mehr als einen Monat. Die größte

[22] Dazu zählen insbesondere Exzellenzen, Professorinnen und Professoren sowie Top-Führungskräfte, die für Vorträge, ausgewählte Projektarbeiten o.ä. in Form von exklusiven Beratungen, Vorträgen o.ä. gewonnen werden.

Verwundbarkeit in Großorganisationen wie der Bundeswehr stellt der einzelne Nutzer dar. Die Sensibilisierung aller Beschäftigten der Bundeswehr hinsichtlich möglicher Cyber-Gefahren, der Informationssicherheit und des persönlichen Datenschutzes wird deshalb künftig über einen jährlich zu aktualisierenden Cyber-Hygiene Check-Up realisiert. Mithilfe eines webgestützten Basis-Moduls wird die bisherige IT-Sicherheitsbelehrung abgelöst und durch ein neues verpflichtendes „Awareness-Verfahren“ zur Erhöhung der allgemeinen Informationssicherheitskompetenz ersetzt. Während sich dieses Basis-Modul an alle Beschäftigten richten wird und auch kurzfristig einsatzbereit ist, sollen darüber hinaus zwei weitere Module für Fachkräfte und Spezialisten entwickelt werden, die höhere Anforderungen enthalten. Ein „advanced“-Modul soll sich an IT-Fachpersonal richten und ein erweitertes Cyber-Verständnis abrufen. Das „professional“-Modul schließlich wird ausschließlich für IT-Spezialisten der Bundeswehr vorgehalten und ruft den Nachweis umfassenden Wissens ab. Dieses Modul wird ausschließlich mit einer zertifizierten Prüfung abzuschließen sein. Den Anfang soll das Ministerium bereits im Mai 2016 mit einem Piloten machen.

Mithilfe des Cyber-Hygiene Check-Up stellt die Bundeswehr sicher, dass die Sensibilisierung für Missbräuche und Risiken der Digitalisierung hohen Qualitätsstandards folgt und zur Verbesserung der Informationssicherheit führt.

Werkstattgespräche „Cyber-Sicherheit“

Die Rolle der Bundeswehr in der gesamtstaatlichen Cyber-Sicherheitsvorsorge war nach der aktuellen Cyber-Sicherheitsstrategie aus dem Jahr 2011 stark auf den Eigenschutz fokussiert. Im engen Dialog mit dem BMI entwickeln die für innere und äußere Sicherheit zuständigen Ministerien jedoch gemeinsam ein neues Verständnis über die intensivere Kooperation und auch Beitragsfähigkeit der Bundeswehr. Dies geschieht auch in Friedenszeiten wie im Rahmen der verfassungsgemäßen Amts- oder Katastrophenhilfe. Um dieses gemeinsame Verständnis von Kooperation und Zusammenarbeit zwischen den verschiedenen Ressortverantwortlichkeiten zu vertiefen, finden bereits Werkstattgespräche zwischen dem BMI und dem BMVg zum Themenkomplex „Cyber-Sicherheit“ statt. Übergreifende Zielsetzung aller Gespräche ist die Identifizierung von gemeinsamen Positionen zu Fragen überlappender Zuständigkeiten, vertiefter strategischer und operativer Kooperation, Synergiepotentialen, möglichen Ansätzen für ihre Umsetzung sowie die gemeinsame Formulierung der aktualisierten Cyber-Sicherheitsstrategie für Deutschland. Die laufenden Gespräche sollen in einen ressortübergreifenden dauerhaften Dialog münden, in den sich die Bundeswehr kontinuierlich einbringt.

Mit der proaktiven, dauerhaften Kooperation und Zusammenarbeit mit anderen Ressorts bei der Aufgabenwahrnehmung in der gesamtstaatlichen Sicherheitsvorsorge bestehen gute Aussichten, die Verfügbarkeit informationstechnischer Systeme bei Cyber-Angriffen und Attacken gegen Staat, Wirtschaft und Gesellschaft übergreifend zu gewährleisten.

7. Nächste Schritte

7.1 Abteilung CIT

Soweit aus den erforderlichen Abstimmungen mit dem BMI, dem BMF und den Personalvertretungen keine derzeit unvorhersehbaren Verzögerungen resultieren, kann die Abteilung CIT in IV/2016 mit einer Grundbefähigung aufgestellt werden. Dabei sind im Zuge der weiteren Arbeiten des Aufbaustabes die notwendigen Abstimmungen zur Bereitstellung der erforderlichen Infrastruktur und des Personals mit priorisierten Verfahren zu gewährleisten.

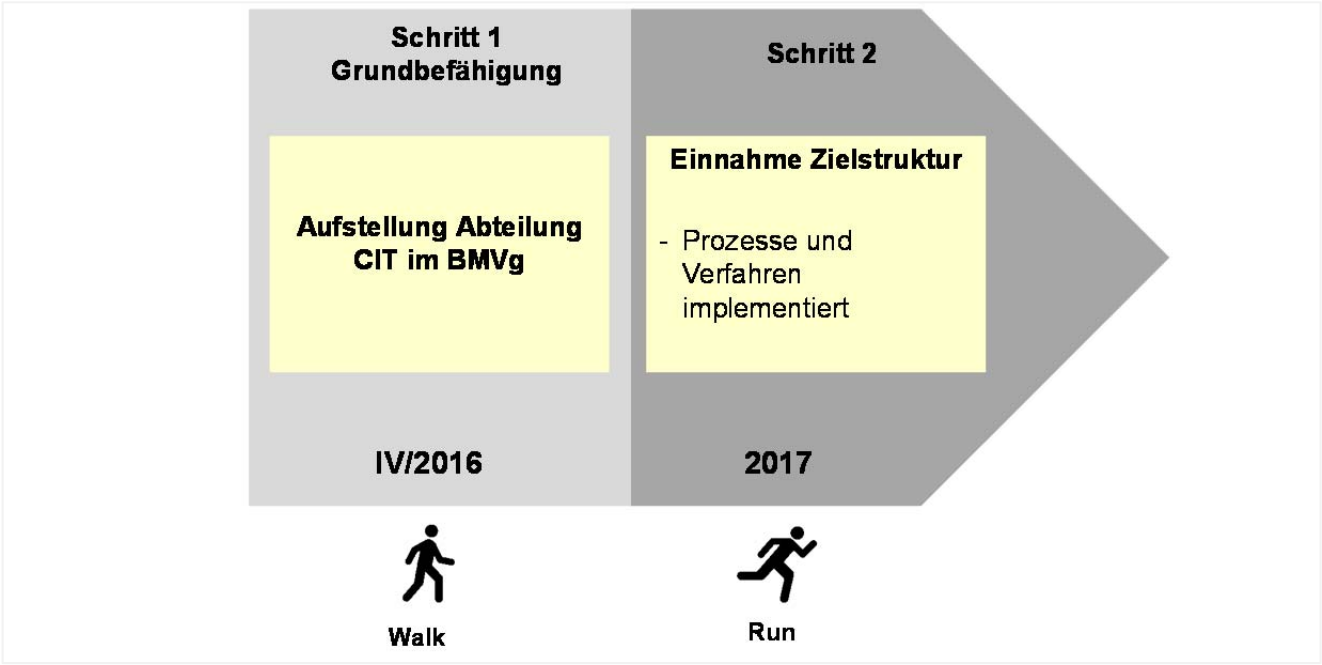

Abbildung 8: Schrittweises Vorgehen zur Aufstellung der Abteilung CIT im BMVg

Unter Berücksichtigung der ganzheitlichen Betrachtung im Rahmen der Organisationsanalyse des BMVg wird die Grundbefähigung der Abteilung in jedem Falle die Steuerung der BWI sowie die weiteren neu abzubildenden Aufgaben gewährleisten. Zusätzlich werden für die Grundbefähigung alle Aufgaben und Ressourcen übertragen, die im Rahmen der Organisationsanalyse nach einer Erstbewertung unkritisch sind. Die Zielstruktur der Abteilung wird im ersten Halbjahr 2017 erreicht.

7.2 Militärischer Organisationsbereich Cyber- und Informationsraum

Sofern in den notwendigen Entscheidungsgängen zur Bereitstellung und Übertragung der Spitzen-/ Dienstposten, des Personals und der Infrastruktur unter Beteiligung der Personalvertretungen keine unvorhersehbaren Verzögerungen auftreten, kann die Erstbefähigung (IOC) KdoCIR zum 01.04.2017 sowie die Übernahme der truppendienstlichen Führungsaufgaben voraussichtlich bis Mitte 2017 erreicht werden. Eine aktive Begleitung der Arbeiten im nachgeordneten Bereich durch den Aufbaustab ist dafür erforderlich.

Für den Zeitraum 2018 bis 2021 sind für den Ausbau des Organisationsbereiches ein Aufwuchs, insbesondere zur Schaffung weiterer fachlicher Mehrwerte, sowie eine Anpassung der Binnenstruktur notwendig. Ab 2021 kann die Zielstruktur (FOC) mit weiteren fachlichen Mehrwerten abhängig von der weiteren Personalentwicklung der Bundeswehr eingenommen werden.

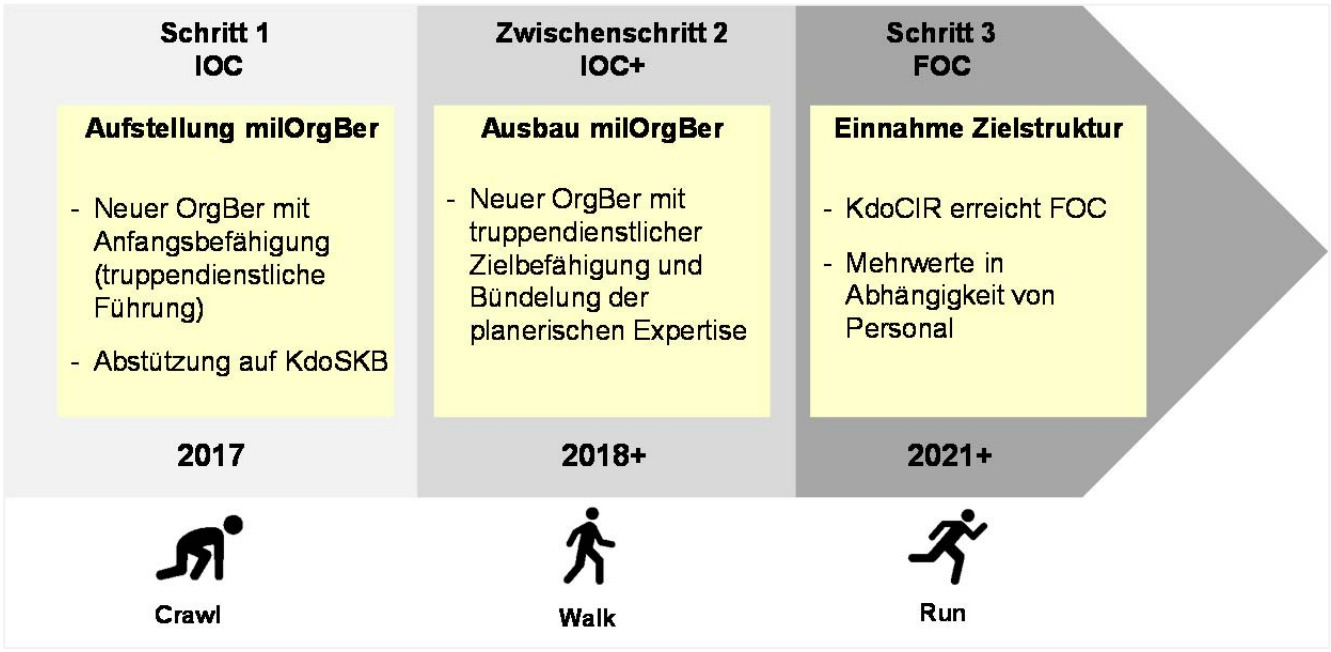

Abbildung 9: Schrittweises Vorgehen zur Aufstellung des Organisationsbereiches CIR

7.3 Fortführung des Aufbaustabs

Die in den Kapiteln 5 und 6 vorgestellten Handlungsempfehlungen sind tiefgreifend für die Bundeswehr. Die zeitgerechte Umsetzung bedarf der Fortführung des Aufbaustabes. Dieser wird sich auf die Aufgabe der weiteren Feinausplanung konzentrieren und eine schnelle, friktionsfreie Realisierung gewährleisten.

Der neue, erweiterte Aufbaustab sollte aus drei Anteilen bestehen:

- einem Leitungselement Bonn/ Berlin,
- einem Anteil CIT für das Organisationselement BMVg mit Sitz in Berlin,
- einem Anteil CIR für den neuen Organisationsbereich CIR mit Sitz in Bonn.

Die beiden Bereiche für CIT und CIR werden von einer Leiterin bzw. einem Leiter Aufbaustab (B7) mit einem eigenen Büro geführt. Dieses wird der für IT zuständigen Staatssekretärin Dr. Suder unterstellt. Der Leiterin bzw. dem Leiter obliegen die zentralen Aufgaben des Veränderungsmanagements CIT und CIR sowie die Innen- und Außenkommunikation gegenüber den eigenen Angehörigen und gegenüber Stakeholdern (parlamentarischer Bereich, Verbände, Industrie, nationale/ internationale Kooperationen und Bündnispartner) bis zur Aufstellung der Abteilung CIT und des KdoCIR.

8. Anlagen

8.1 Abkürzungsverzeichnis

AA	Auswärtiges Amt
AIN	Ausrüstung, Informationstechnik und Nutzung
APT	Advanced Persistant Threat
AuswZ EloKa	Auswertezentrale Elektronische Kampfführung
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BB-8 Droid	Unterstützungskraft für den InspCIR
BITS	Betriebszentrum IT-System der Bundeswehr
BMI	Bundesministerium des Inneren
BMVg	Bundesministerium der Verteidigung
Bw	Bundeswehr
BWI	Bundeswehr Informationstechnik GmbH
CERTBw	Computer Emergency Response Team der Bundeswehr
CGM	Commercial, Government, Military Off the Shelf
CC	Component Command
C-IED	Counter-Improvised Explosive Device
CIO	Chief Information Officer
CIR	Cyber- und Informationsraum
CISO	Chief Information Security Officer
CISOBw	Chief Information Security Officer der Bundeswehr
CIT	Cyber/ IT
CNO	Computer Netzwerk Operationen
COI	Community of Interests
CPM (nov.)	Customer Product Management (novelliert)
DDoS	Distributed Denial of Service
DP	Dienstposten
EloKa	Elektronische Kampfführung
F&T	Forschung und Technologie
FOC	Full Operating Capability
FüSK	Führung Streitkräfte
FüUstgKdoBw	Führungsunterstützungskommando der Bundeswehr
GeoInfoDBw	Geoinformationsdienst der Bundeswehr

GeoInfoWBw	Geoinformationswesen der Bundeswehr
GIS	Geoinformationssystem
GPS	Global Positioning System
IFG	Informationsfreiheitsgesetz
Insp	Inspekteur/ Inspekteurin
IOC	Initial Operating Capability
IPP	Integrierter Planungsprozess
IT	Informationstechnik
ITE	Informationstechnik und Elektronik
IT-SysBw	IT-System der Bundeswehr
IT-ZentrumBw	Zentrum für Informationstechnik der Bundeswehr
IUD	Infrastruktur, Umwelt und Dienstleistungen
Kdo	Kommando
KdoITBw	Kommando Informationstechnik der Bundeswehr
KdoStratAufkl	Kommando Strategische Aufklärung
LAN	Local Area Network
LP	Leistungsprozess
LPV	Leistungsprozessverantwortliche/ Leistungsprozessverantwortlicher
MilNW	Militärisches Nachrichtenwesen
MilOrgBer	Militärischer Organisationsbereich
MINT	Mathematik, Ingenieurwissenschaften, Naturwissenschaften und Technik
NATO	North Atlantic Treaty Organization
OrgBer	Organisationsbereich
OpKom	Operative Kommunikation
PE	Prozesseigner
PIZ	Presse- und Informationszentrale
PoC	Point of Contact
Plg	Planung
SASPF	Standard-Anwendungs-Software-Produkt-Familien
SE	Strategie und Einsatz
SiN	Systeme in Nutzung
StvInsp	Stellvertretender Inspekteur/ Stellvertretende Inspekteurin
TP	Teilprozess
TSK	Teilstreitkraft

UniBw	Universität der Bundeswehr
ZCO	Zentrum Cyber-Operationen
ZCSBw	Zentrum Cyber-Sicherheit der Bundeswehr
ZOpKomBw	Zentrum Operative Kommunikation der Bundeswehr

8.2 Abbildungsverzeichnis

8.3 Bezugsdokumente

1. Kabinettsbeschluss IT-Steuerung Bund vom 05.12.2007
2. Bundesministerium der Verteidigung, Bundesministerin, Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg vom 16.04.2015
3. Kabinettsbeschluss Grobkonzept zur IT-Konsolidierung Bund vom 20.05.2015
4. Bundesministerium der Verteidigung, Bundesministerin, Tagesbefehl vom 17.09.2015
5. Bundesministerium der Verteidigung, Bundesministerin, Innenverteiler III vom 01.11.2015
6. Bundesministerium der Verteidigung, Staatssekretär Hoofe, Innenverteiler III vom 11.11.2015
7. Bundesministerium der Verteidigung, Staatssekretärin Dr. Suder, IT-Strategie des Geschäftsbereichs BMVg vom 02.12.2015

8.4 Definitionen

Advanced Persistent Threat (APT)

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten (dauerhaften) Zugriff zu einem Opfernetzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.[23]

Cyber-Abwehr

Cyber-Abwehr ist der Teil der Cyber-Verteidigung, der alle ausschließlich defensiven Maßnahmen umfasst, die zur Einsatz- und Operationsführung geeignet sind oder dem Schutz eigener Informationen, IT sowie Waffen- und Wirksysteme dienen.[24]

Cyber-Angriff

Ein Cyber-Angriff ist ein IT-Angriff im Cyber-Raum, der sich gegen einen oder mehrere andere IT-Systeme richtet und zum Ziel hat, die IT-Sicherheit zu brechen. Die Ziele der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit können dabei als Teil oder Ganzes verletzt sein.[25]

Ein Cyber-Angriff im Verständnis des Geschäftsbereiches BMVg ist jede bewusste Handlung mit informationstechnischen Mitteln im, aus und auf den Cyber-Raum, die geeignet ist, die eigene Einsatz- und Operationsführung zu stören und zu beeinflussen oder die Verfügbarkeit, Integrität oder Vertraulichkeit eigener Informationen, IT sowie Waffen- und Wirksysteme zu gefährden.[26]

Cyber-Außenpolitik

Cyber-Außenpolitik ist eine Querschnittsaufgabe mit Auswirkungen auf fast alle Politik- und Handlungsfelder der Außenpolitik. Ziel dieser Politik ist es, die wirtschaftlichen Chancen des Internets auszubauen, universelle Menschenrechte wie den Schutz der Privatsphäre und Meinungs- und Pressefreiheit auch im Internet zu schützen und die freiheitsstiftenden Wirkungen des Internets verantwortungsvoll zu nutzen, sowie die Sicherheit des Cyberraum zu gewährleisten und aus der zunehmenden Digitalisierung entstehende Bedrohungen einzudämmen.[27]

[23] Bundesamt für Sicherheit in der Informationstechnik 2015. Die Lage der IT-Sicherheit in Deutschland 2015, S. 50.
[24] Bundesministerium der Verteidigung 2015. Entwurf Umsetzungsstrategie Cyber-Verteidigung, S. 34.
[25] Bundesministerium des Innern 2011. Cyber-Sicherheitsstrategie für Deutschland, S. 14-15.
[26] Bundesministerium der Verteidigung 2015. Entwurf Umsetzungsstrategie Cyber-Verteidigung, S. 34.
[27] Auswärtiges Amt 2015. Cyber-Außenpolitik, URL: http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik_node.html, Stand 13.11.2015.

Cyber Defence

Cyber Defence umfasst die präventiven und reaktiven Maßnahmen zur Abwehr von Cyber-Angriffen auf in IT-Systemen verarbeitete, gespeicherte oder übertragene Informationen oder auf diese IT-Systeme selbst bzw. deren Steuerinformationen, einschließlich der Maßnahmen zur Wiederherstellung der Cyber-Sicherheit nach erfolgreichen Cyber-Angriffen.[28]

Cyber-Hygiene

Cyber-Hygiene bezeichnet alle grundlegenden und regelmäßigen Maßnahmen, die der Erhöhung der Sensibilisierung des einzelnen Nutzers hinsichtlich der Gefahren aus dem Cyber-Raum sowie der Pflege und Aktualisierung der Systeme dienen und damit die Grundlage für die Cyber-Sicherheit bilden.

Cyber-Operationen

Cyber-Operationen umfassen alle offensiven und defensiven Maßnahmen, die zur Einsatz- und Operationsführung geeignet sind oder dem Schutz eigener IT sowie Waffen- und Wirksysteme dienen.[29]

Cyber-Raum

Der Cyber-Raum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber-Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann. IT-Systeme in einem isolierten virtuellen Raum sind kein Teil des Cyber-Raums.[30]

Für den Geschäftsbereich BMVg wird diese Definition erweitert um den Anteil der IT-Systeme, die über Datenschnittstellen verfügen, ansonsten aber von öffentlich zugänglichen Netzen und dem Internet separiert sind.[31]

Cyber- und Informationsraum

Im Zentrum der Dimension Cyber- und Informationsraum steht die Information. Diese wird im Informationsumfeld durch Menschen wahrgenommen und interpretiert. Der Cyber-Raum ist in das Informationsumfeld eingebettet und ermöglicht die (teil)automatisierte Verarbeitung und Verbreitung von Informationen.[32] Er umfasst über territoriale und strukturelle Grenzen hinweg alle über das Internet und sonstige Netze auf Datenebene vernetzte oder über Datenschnittstellen erreichbare Informationssys-

[28] Bundesministerium der Verteidigung 2015. Entwurf Umsetzungsstrategie Cyber-Verteidigung, S. 34.
[29] Bundesministerium der Verteidigung 2015. Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich des BMVg, S. 14.
[30] Bundesministerium des Innern 2011. Cyber-Sicherheitsstrategie für Deutschland, S. 14-15.
[31] Bundesministerium der Verteidigung 2015. Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich des BMVg, S. 5.
[32] vgl. Bundesministerium der Verteidigung 2013. Konzeption der Bundeswehr, S. 35.

teme. Das elektromagnetische Spektrum ist ein wesentliches Trägermedium von Kommunikation im Cyber-Raum und Informationsumfeld.

Cyber-Sabotage

Cyber-Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems werden als Cyber-Sabotage bezeichnet.[33]

Cyber-Sicherheit

Cyber-Sicherheit in Deutschland ist der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des deutschen Cyber-Raums auf ein tragbares Maß reduziert sind.[34]

Cyber-Sicherheit ist der anzustrebende Zustand der IT-Sicherheitslage, in dem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind.[35]

Cyber-Spionage

Cyber-Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden, wenn sie von fremden Nachrichtendiensten ausgehen oder gesteuert werden, als Cyber-Spionage, ansonsten als Cyber-Ausspähung bezeichnet.[36]

Cyber-Verteidigung

Die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyber-Raum, die zur Einsatz- und Operationsführung geeignet sind oder zur Abwehr von Cyber-Angriffen und damit dem Schutz eigener Informationen, IT sowie Waffen- und Wirksysteme dienen, werden unter diesem Begriff zusammengefasst. Dazu zählen Gewährleistung der IT-Sicherheit, Cyber Defence, Computer Netzwerk Operationen und IT-Abschirmung.[37]

Cyber-Verteidigungspolitik

Cyber-Verteidigungspolitik ist die Wahrung der äußeren Sicherheit Deutschlands und seiner Verbündeter auch im Cyber-Raum.

[33] Bundesministerium des Innern 2011. Cyber-Sicherheitsstrategie für Deutschland, S. 14-15.
[34] Bundesministerium des Innern 2011. Cyber-Sicherheitsstrategie für Deutschland, S. 14.
[35] Bundesministerium der Verteidigung 2015. Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich des BMVg, S. 6.
[36] Bundesministerium des Innern 2011. Cyber-Sicherheitsstrategie für Deutschland, S. 14-15.
[37] vgl. Bundesministerium der Verteidigung 2015. Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich des BMVg, S. 4.

Hybride Bedrohung

Hybride Bedrohung ist das Umsetzen einer hybriden Strategie durch einen staatlichen oder nichtstaatlichen Akteur. Die hybride Strategie basiert dabei auf einer breiten, komplexen, anpassbaren und meistens hoch integrierten Kombination von konventionellen und/ oder unkonventionellen Mitteln, offener und/ oder verdeckter Aktivitäten von militärischen, paramilitärischen und/ oder zivilen Akteuren, durchgeführt im gesamten Fähigkeitsspektrum gezielt ausgerichtet auf die Entscheidungsfindung und das Erschweren eigener Aktivitäten[38].

IT-Krise

Eine IT-Krise liegt dann vor, wenn trotz der vorbeugenden Maßnahmen in der Behörde/im Ressort/in der Nation eine vom Normalzustand abweichende Situation eintritt, die mit der normalen Aufbau- und Ablauforganisation nicht bewältigt werden kann.[39]

Krise

Eine vom Normalzustand abweichende Situation mit dem Potential für oder mit bereits eingetretenen Schäden an Schutzgütern, die mit der normalen Aufbau- und Ablauforganisation eines Staates nicht mehr bewältigt werden kann.[40]

Kritische Infrastrukturen (KRITIS)

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten.

In Deutschland werden folgende Sektoren (und Branchen) den Kritischen Infrastrukturen zugeordnet:

- Transport und Verkehr (Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
- Energie (Elektrizität, Mineralöl, Gas)
- Informationstechnik und Telekommunikation (Telekommunikation, Informationstechnik)
- Finanz- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister, Börsen)
- Staat und Verwaltung (Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall- und Rettungswesen einschließlich Katastrophenschutz)

[38] vgl. NATO RESTRICTED, PO(2015)0673 - Strategy on NATO's Role in Countering Hybrid Warfare, S. 1.
[39] VS-NfD, Bundesministerium des Innern 2011. IT-Krisenmanagement bei IT-Krisen mit Auswirkungen auf die Bundesverwaltung: Teil I – Strukturen in IT-Krisen, S. 5.
[40] VS-NfD, Bundesministerium des Innern 2011. IT-Krisenmanagement bei IT-Krisen mit Auswirkungen auf die Bundesverwaltung: Teil I – Strukturen in IT-Krisen, S. 5.

- Ernährung (Ernährungswirtschaft, Lebensmittelhandel)
- Wasser (Öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung)
- Gesundheit (Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore)
- Medien und Kultur (Rundfunk - Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke)[41]

Recognized Environmental Picture

Das Recognized Environmental Picture ist eine umfassende ebenengerechte, in sich konsistente Darstellung von Geofaktoren und deren einsatzrelevante Bewertung für Planung, Durchführung und Nachbereitung militärischer Operationen und einsatzgleicher Verpflichtungen. Es stellt qualitätsgeprüfte, bewertete und zur Nutzung freigegebene Geoinformationen eines Raumes zur Verfügung und trägt damit entscheidend zur Erzeugung eines Gemeinsamen Rollenorientierten Einsatzlagebildes bei.

Resilienz

Resilienz wird oft als Widerstandsfähigkeit übersetzt – das Konzept geht jedoch darüber hinaus. Resilienz beschreibt einerseits die Fähigkeit eines Systems, nach einem externen Schock in den Ursprungszustand zurückzukehren, d.h. sich zu „erholen“ (recovery). Andererseits kann Resilienz auch bedeuten, dass ein durch einen externen Schock beeinträchtigtes und verändertes System seine Kernaufgaben weiterhin erfüllt, indem es sich dem Ereignis entsprechend anpasst (adaptation).[42]

Resilienz ist die Fähigkeit eines Systems, mit Veränderungen umgehen zu können. Resilienz bedeutet Widerstandsfähigkeit gegen Störungen jeder Art, Anpassungsfähigkeit an neue Bedingungen und eine flexible Reaktion auf Veränderungen mit dem Ziel, das System – z. B. einen Betrieb oder einen Prozess – aufrecht zu erhalten.[43]

[41] Bundesministerium des Innern 2009. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), S. 3.
[42] vgl. Giroux, Jennifer & Prior, Tim 2012. Expressions of Resilience: From "Bounce Back" to Adaptation. 3RG Report. Zürich: Center for Security Studies, S. 5.
[43] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2016. Glossar. URL: http://www.bbk.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functions/glossar.html?lv2=4968608, Stand: 25.02.2016