



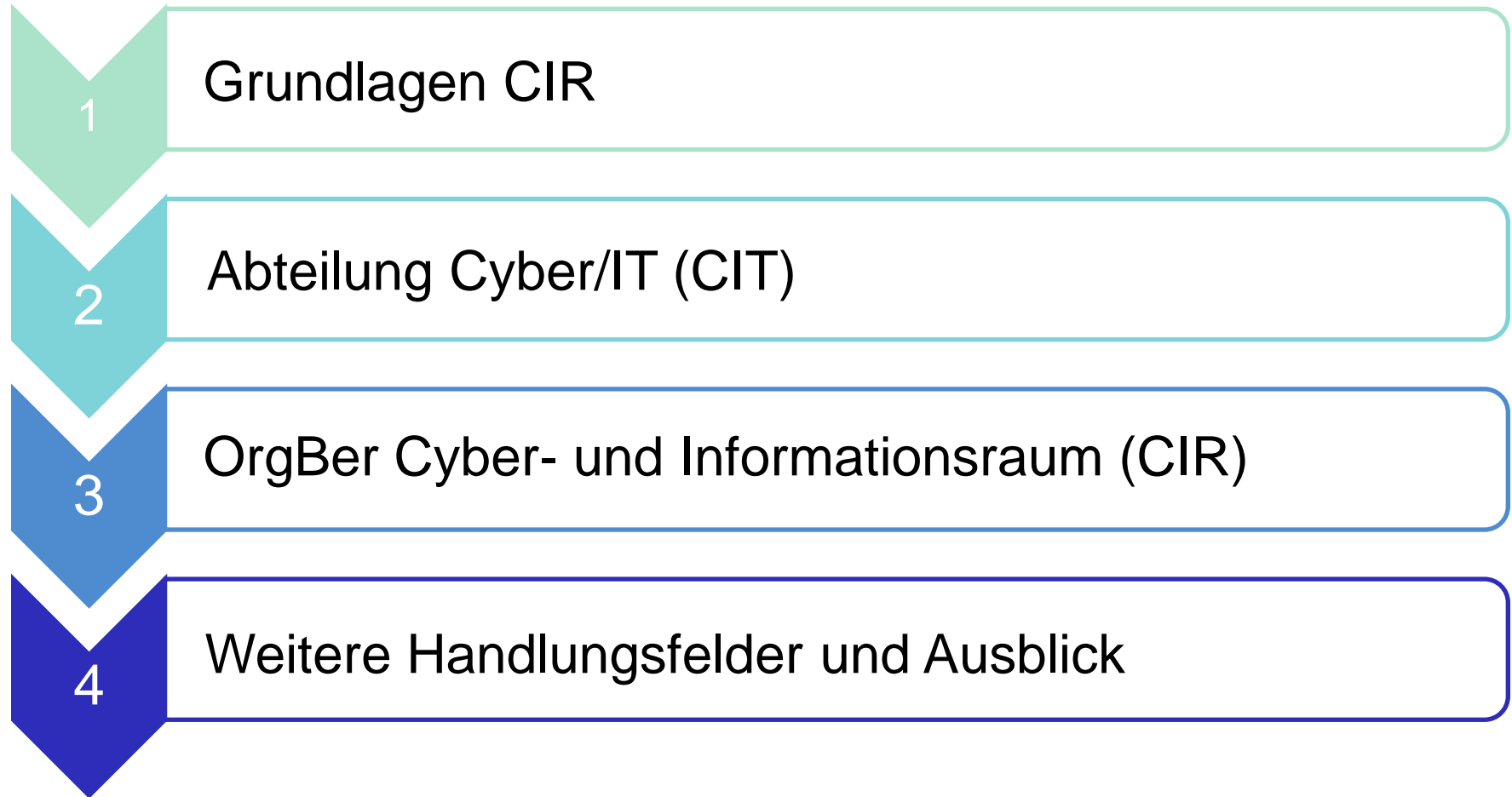
Perspektiven und Herausforderungen im zukünftigen OrgBer Cyber- und Informationsraum (CIR)

Oberst i.G. Fleischmann

ChdSt Aufbaustab Cyber- und Informationsraum



Gliederung





1

Grundlagen CIR

2

Abteilung Cyber/IT (CIT)

3

OrgBer Cyber- und Informationsraum (CIR)

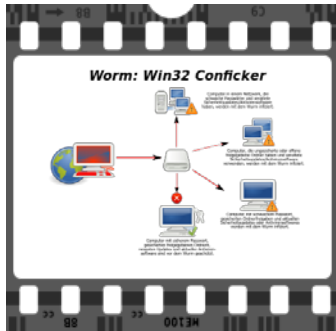
4

Weitere Handlungsfelder und Ausblick



Ausgangslage - Auswahl aufgedeckter Cyber-Angriffe -

CONFICKER



2008

STUXNET



2010

E-Mail
Diebstahl



2013

US CENTCOM



2015

TV5
MONDE



2015

Bundestag
(APT28)



2015

Fall Lisa



2016



International



- **NATO: Enhanced NATO Policy on Cyber Defence**



- **EU: Politikrahmen für die Cyberabwehr**

National

- **BMI: Cyber-Sicherheitsstrategie Deutschland**



Bundesministerium
des Innern

- **BMVg: Strategische Leitlinie Cyber-Verteidigung**

- **BMVg: IT-Strategie**



Bundesministerium
der Verteidigung

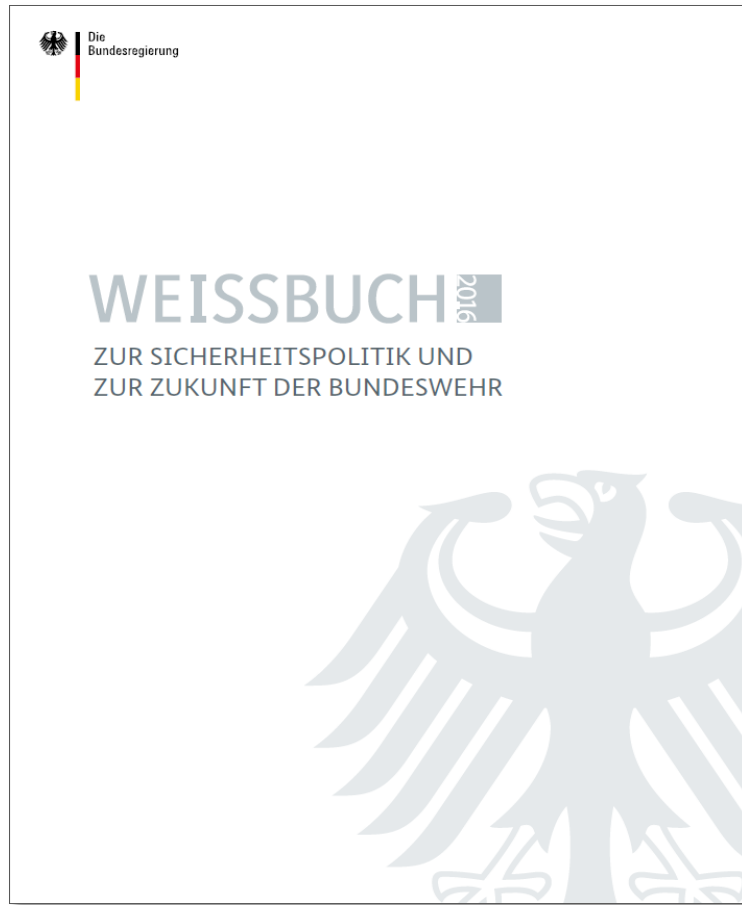
- **Weißbuch 2016**

WEISSBUCH 2016
Zur Sicherheitspolitik und zur Zukunft der Bundeswehr



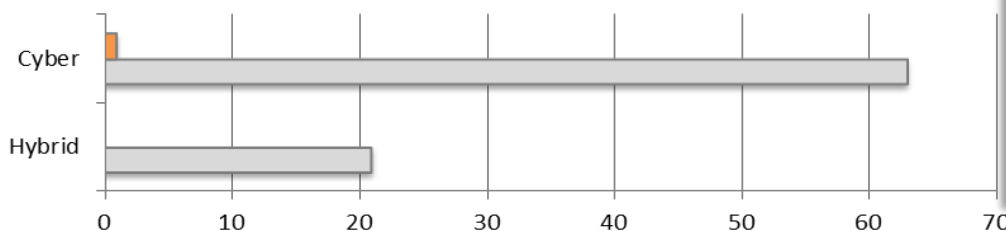
Weißbuch 2016 (13.07.2016)

Auswirkungen auf die Bw im Bereich CIR



- Gesamtstaatliche Fähigkeiten ausbauen, also ressortübergreifend kooperieren und mit Wissenschaft, Industrie und Partnern vernetzen.
- Bundeswehreigene Cyberfähigkeiten ausbauen, dabei Sicherheitsarchitektur des IT-Systems der Bw konsolidieren und resilienter machen.
- Waffensysteme und Gefechtsstände sowie Lieferketten in der Rüstung härten
- Spitzenpersonal durch Schaffung attraktiver Cyberkarrierepfade und innovativer Personalgewinnungsstrategien rekrutieren
- Fragmentierte Zuständigkeiten und Strukturen für einen robusten Fähigkeitsaufbau zusammenführen, die IT-Fähigkeiten bündeln sowie zentrale Ansprechpartner für andere Ressorts und multinationale Partner schaffen.

Häufigkeit der Nennungen (■ WB 2006 / ■ WB 2016):





Cyber-Sicherheitsstrategie für Deutschland 2016 (09.11.2016)

Auswirkungen für die Bundeswehr

- **Deutlich stärkere Rolle der Bundeswehr in der gesamtstaatlichen Sicherheitsvorsorge**
- **Schutz Kritischer Infrastrukturen ressortgemeinsame Aufgabe**
- **Auf- und Ausbau eines Cyber-Cluster bei UniBw M**
- **Weiterentwicklung des NCAZ**
- **Bw Incident Response Teams Teil der gesamtstaatlichen Sicherheitsvorsorge (Amtshilfe)**
- **Intensivierung der Zusammenarbeit nationaler CERT Strukturen**
- **Aufbau einer Cyber-Reserve in der Bw**
- **Cyber-Raum ist Operationsraum (analog NATO)**





Technologie Kontext

- Cyber- und Informationsraum wird Konflikte der Zukunft maßgeblich bestimmen
 - IT determinierend
 - Bedrohung im Cyber Raum (Staat, Terror, Hacker)
- Schnellebigkeit IT
 - Innovationen vom Markt schneller in die operationelle Nutzung überführen
 - Anpassung Entscheidungs- und Beschaffungszeiten mit dem Ziel der Verkürzung



Gliederung

1

Grundlagen CIR

2

Abteilung Cyber/IT (CIT)

3

OrgBer Cyber- und Informationsraum (CIR)

4

Weitere Handlungsfelder und Ausblick

Entscheidung Verteidigungsministerin

Tagesbefehl vom 05.10.2016



Die Bundesministerin Berlin, 5. Oktober 2016

Tagesbefehl

Soldatinnen und Soldaten,
zivilen Mitarbeiterinnen und Mitarbeiter!

Als offene Gesellschaft und global vernetzte Volkswirtschaft stehen wir vor einschneidenden sicherheitspolitischen Herausforderungen. Gefahren, Konflikte und Krisen entwickeln sich dynamischer, sie treten parallel auf, wirken auf unterschiedlichen Ebenen und beeinflussen sich wechselseitig. In dieser Situation haben wir den Cyber- und Informationsraum als eine Dimension identifiziert, der wachsende Bedeutung zukommt. Um eine verantwortungsvolle gesamtstaatliche Sicherheitskonzepte zu gewährleisten, muss auch der Geschäftsbereich des Bundesministeriums der Verteidigung seine Kompetenzen und Fähigkeiten langfristig auf die neuen Herausforderungen hin ausrichten.

Der Cyber- und Informationsraum hat sich bei unseren Partnern und Verbündeten längst zu einem strategischen Handlungsfeld entwickelt, mit dem Diktat von Wertschau gilt er offiziell als militärischer Operationsraum der NATO. Für die Bundeswehr heißt das: Sie muss Schritt halten mit dieser Entwicklung. Sie muss das Thema intensiv besitzen und damit gestalten. Sie muss die mit der Digitalisierung verbundenen Chancen nutzen, aber auch frühzeitig die Risiken erkennen – und Gefahren wirkungsvoll begegnen können. Zudem muss die Bundeswehr in der Lage sein, sich auf länger werdende technische Innovationszyklen in der Informations- und Kommunikationstechnik einzustellen.

Mit meiner Entscheidung vom 28. April 2016 habe ich den erweiterten Aufbaustab „Cyber- und Informationsraum“ (CIR) unter der Führung von Herrn Generalmajor Leitner anwesend, die notwendigen organisatorischen Veränderungen im Ministerium und im nachgeordneten Bereich vorzubereiten.

Mit dem heutigen Tag ist ein erster Meilenstein dieser Arbeiten erreicht. Wir richten im Ministerium – an den Standorten Bonn und Berlin – die neue Abteilung Cyber/IT (CTI) ein. Mit deren Führung habe ich Herrn Klaus-Hardy Mühleck betraut. Er verantwortet in dieser Funktion künftig die Bereiche Cyber-IT-Governance und IT-Service/Informationssicherheit sowie die zukünftige strategisch inhaltliche Ausrichtung der Bundeswehr Informationstechnik GmbH (BWIT). Zugleich nimmt der Abteilungsleiter die Aufgaben des „Chief Information Officer“ für unser Ressort wahr.

In der neuen Abteilung bündeln wir alle IT- und cyber-relevanten Aufgaben und Fähigkeiten an einer zentralen Stelle im Ministerium. Dazu werden bestimmte Dienstposten verschoben, aus dem Aufbaustab, aber auch aus anderen Referaten; so dass sich Unterstellungen ändern. Das wiederum hat zur Folge, dass die bisherige Abteilung Ausrüstung, Informationstechnik und Nutzung (AIN) nach der Ausgliederung des IT-Anteils nun umbenannt wird in Abteilung Ausrüstung (A).

Mit dieser organisatorischen Weiterentwicklung beginnen wir, auf der Ebene des BMVg die entscheidenden Weichen zu stellen für eine stärker IT-getriebene Modernisierung sowie die Aufwertung des Cyber- und Informationsraumes zu einer eigenständigen militärischen Dimension. Und wir bauen damit ganz konkret unseren Beitrag für eine umfassende Sicherheitsarchitektur in Deutschland aus.

Für das außerordentliche Engagement, mit dem alle Beteiligten diese wichtigen Schritte in die Zukunft gestaltet und vorangetrieben haben, möchte ich mich von Herzen bedanken. Ich wünsche Herrn Mühleck und seinen Mitarbeiterinnen und Mitarbeitern viel Erfolg für die herausfordernde Arbeit. Und ich bin mir sicher, dass wir auch die nächsten Etappen auf diesem Weg gemeinsam meistern werden.

Ursula von der Leyen
Dr. Ursula von der Leyen
Bundesministerin der Verteidigung

Kernaussagen

- **Erster Meilenstein** des erweiterten Aufbaustabes CIR erreicht.
- Einrichten einer neuen **Abteilung Cyber/IT im BMVg in BERLIN und BONN** mit **Klaus-Hardy Mühleck** als Abteilungsleiter CIT und Ressort Chief Information Officer.
- Weichenstellung für **stärker IT-getriebene Modernisierung** und **Aufwertung CIR** zu einer **eigenständigen militärischen Dimension**.

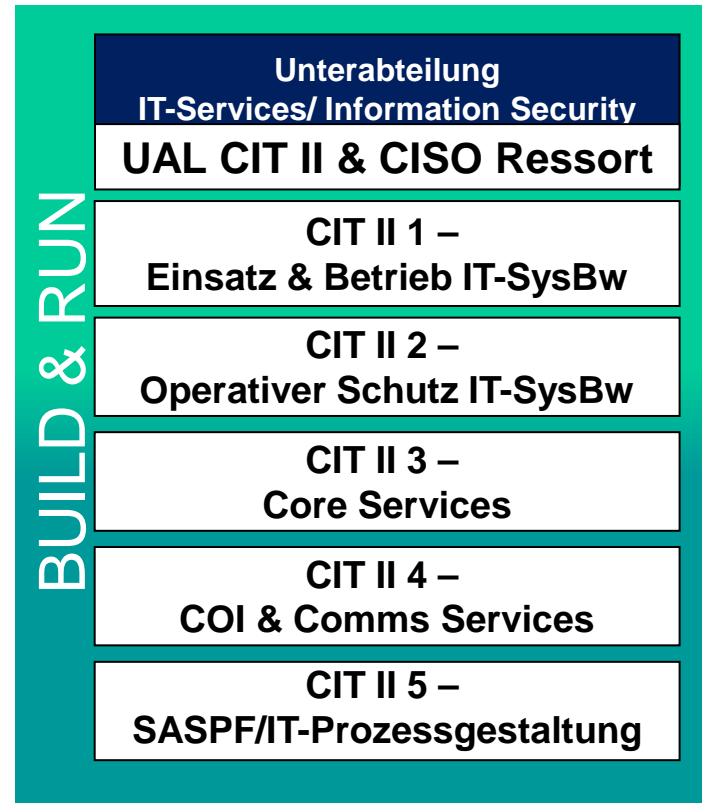




Abteilung Cyber/IT im BMVg

**Abteilung
Cyber/ IT (CIT)**
Abteilungsleiterin/ Abteilungsleiter CIT
& Ressort-CIO

CIT BWI
Inhaltlich-strategische
Steuerung BWI



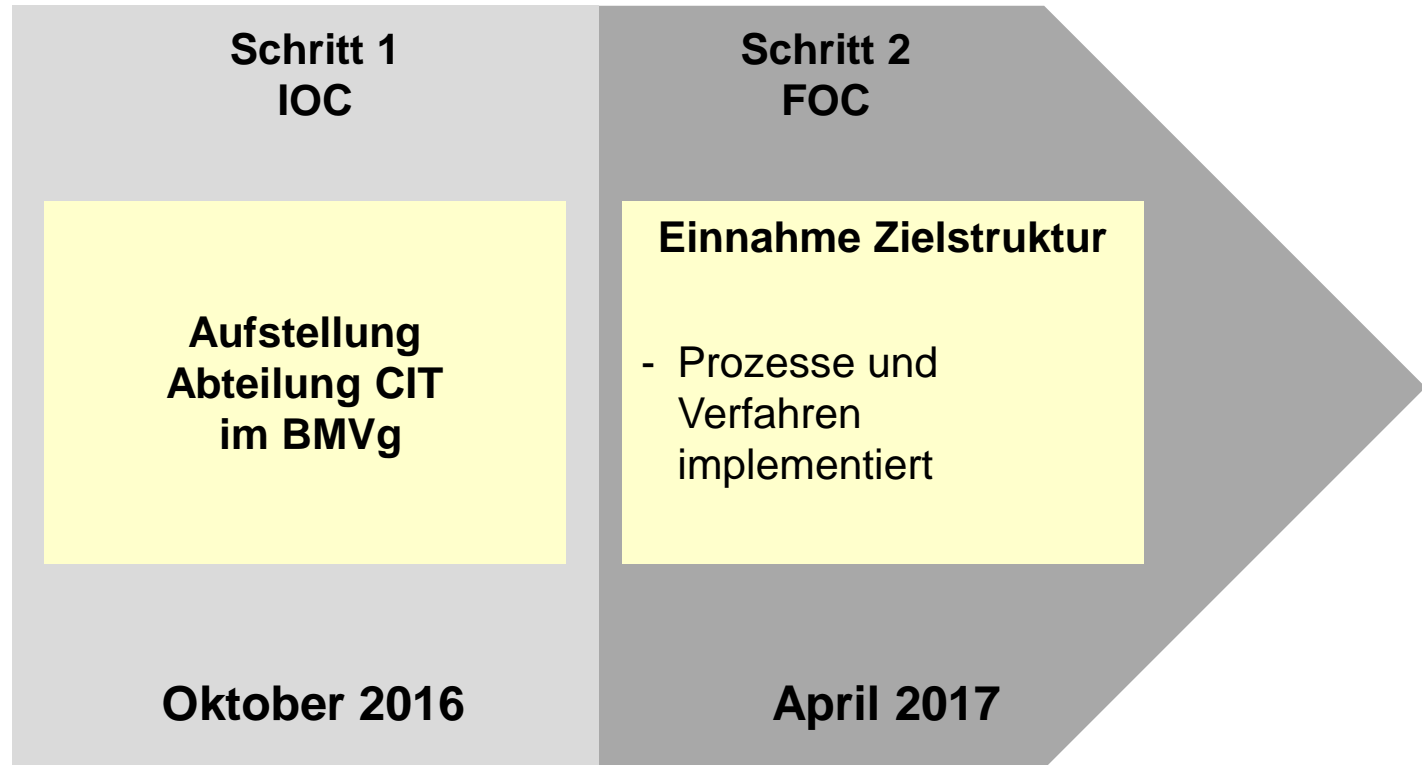
 Dienstsitz Berlin

 Dienstsitz Bonn

Ziel: **Klare Zuständigkeiten** im Bereich Cyber/IT (Planung/Beschaffung/Betrieb) und Abteilung SE (Einsatz)



Stufenweise Umsetzung der Abteilung Cyber/IT



Walk

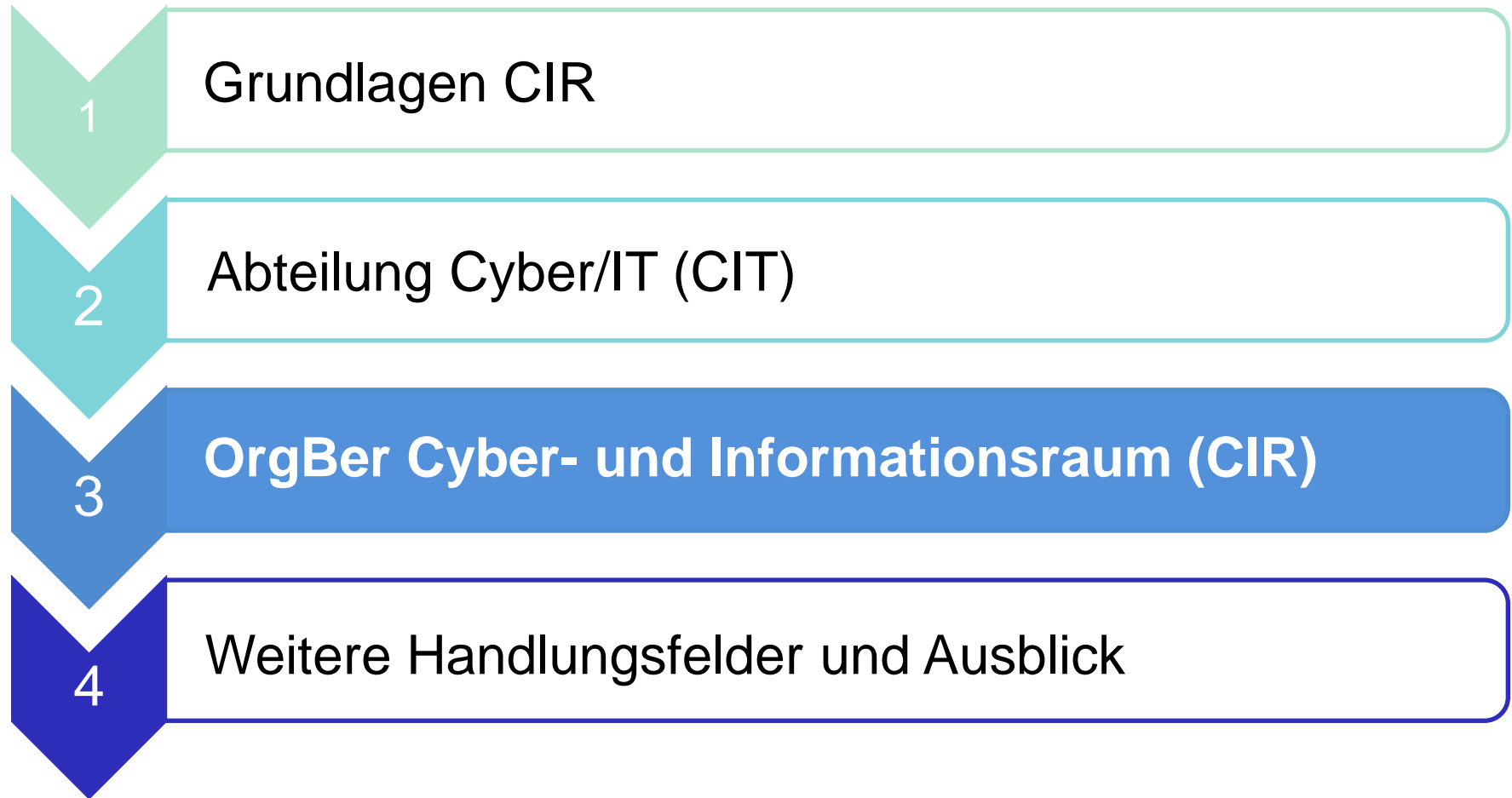


Run

Status: Alle Arbeiten im Zeitplan!

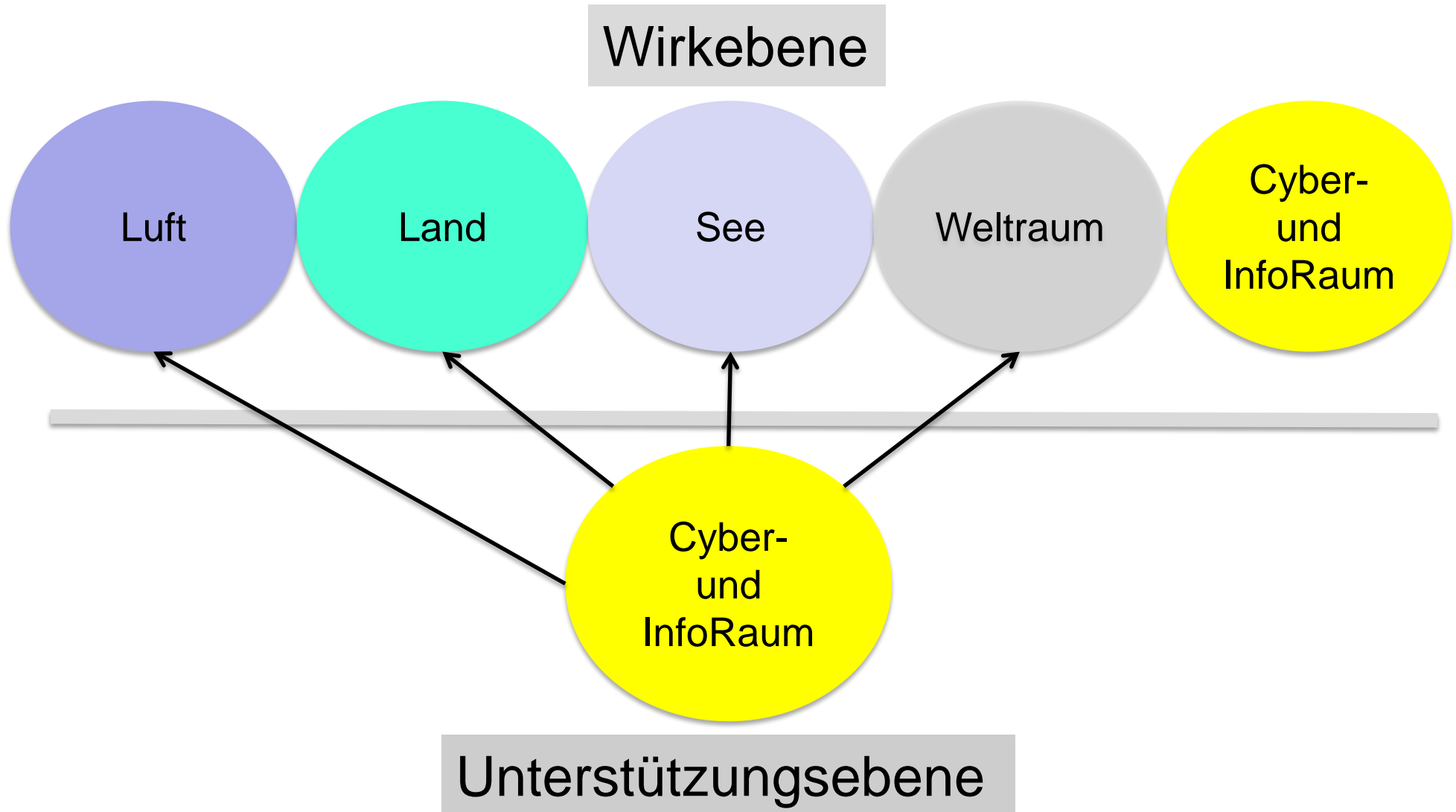


Gliederung





Dimension Cyber- und Informationsraum





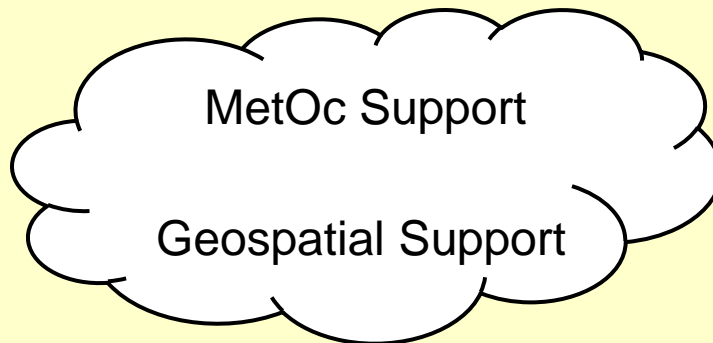
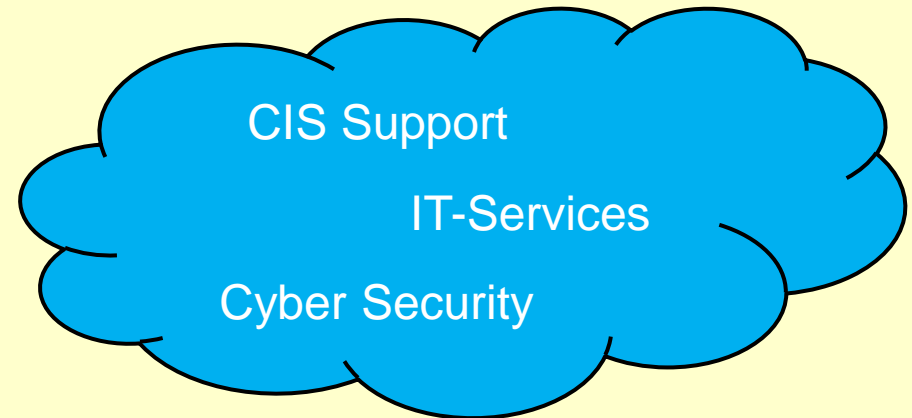
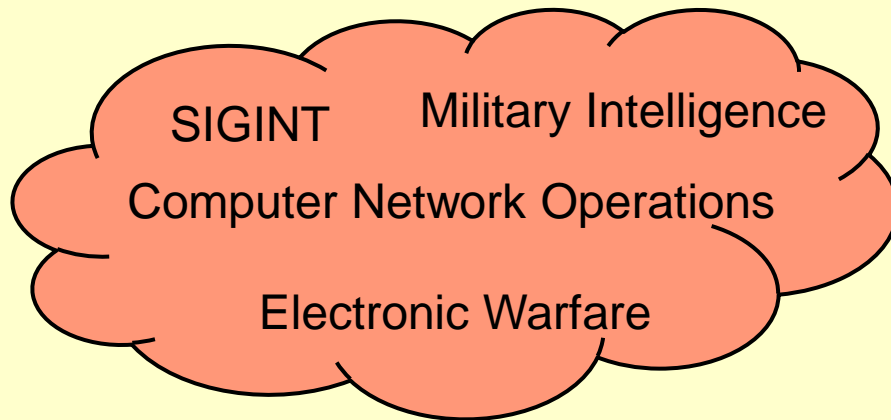
CIR der Orgbereich für die Dimension Cyber- und Informationsraum

- Vergleichbare Zuständigkeiten wie Heer, Luftwaffe und Marine für die Dimensionen Land, Luft, Weltraum und See
- Aufbau von neuen und Weiterentwicklung von vorhandenen Fähigkeiten in der Dimension CIR für alle OrgBer
- Wesentliche Säulen
 - Schutz und Betrieb des IT-Systems der Bundeswehr (Neue Dauereinsatzaufgabe)
 - Aufklärung und Wirkung im CIR (elektromagnetisches Spektrum, Informations- und Kommunikationstechnik und Informationsumfeld)
 - GeoInfo-Unterstützung als Enabler (u.a. Raumbezug als Basis und Scharnier zwischen CIR und anderen Dimensionen)
- Stellt bereit in der Domäne Wirkung die nicht kinetischen Optionen und Beiträge der Bundeswehr im Cyber- und Informationsraum im Rahmen des gesamtstaatlichen Krisenmanagements bis zur Landes- und Bündnisverteidigung sowie bei Auslandseinsätzen



CIR-relevante Fähigkeiten werden zusammengeführt

Cyber-/Informationsraum



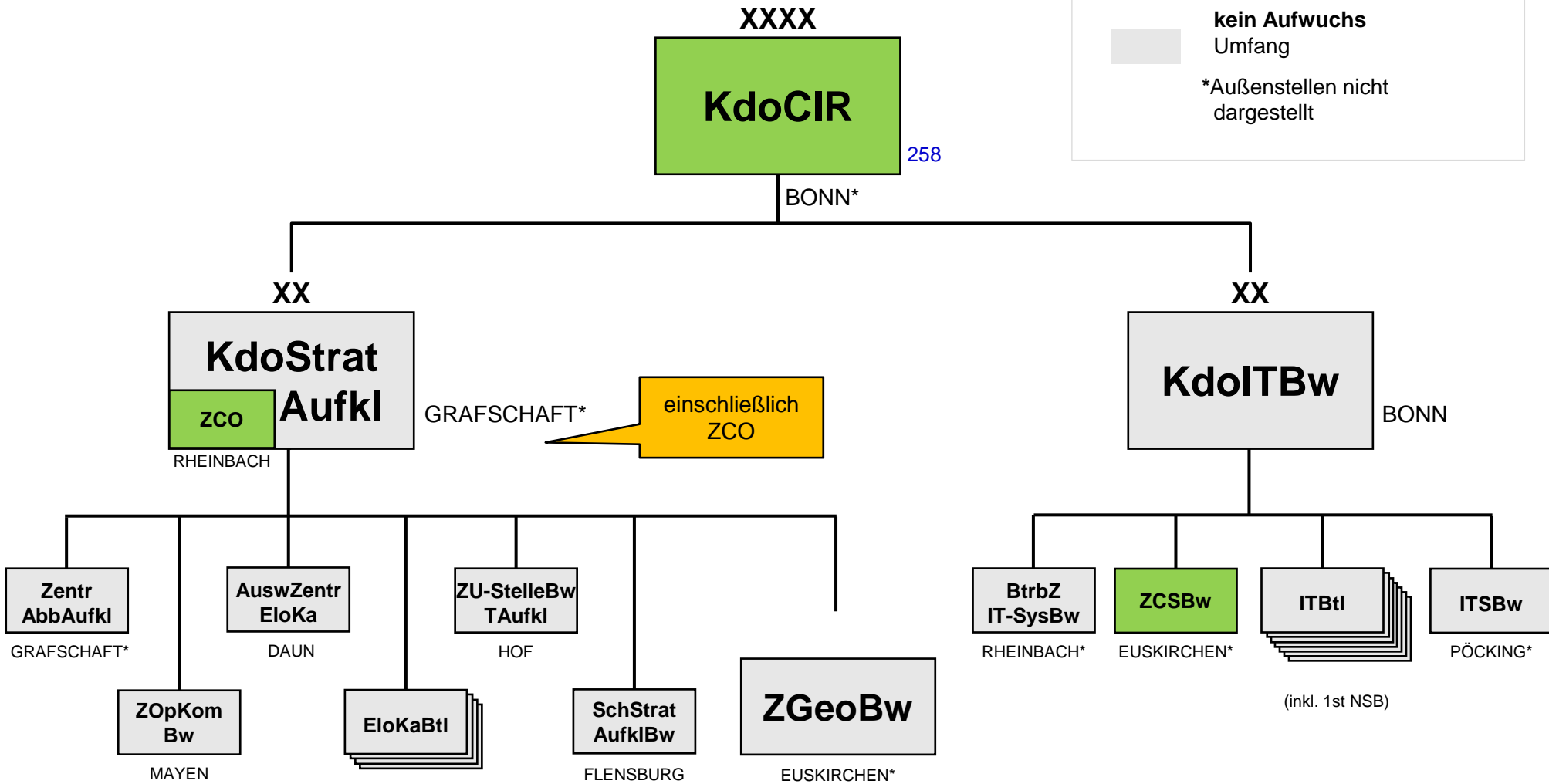
Ziel: Synergie unterschiedlicher Fähigkeiten und bessere Verzahnung bei “mission preparation and execution”



OrgBer CIR 2017 IOC

Legende:

- Aufwuchs**
- kein Aufwuchs**
Umfang
- *Außenstellen nicht dargestellt





Ausbau Stab KdoCIR und weitere Stärkung der Fähigkeiten im Bereich CIR

Zentrum Cybersicherheit Bundeswehr



- Verbesserter Schutz des eigenen CIR, durchhaltefähig (24/7)
- Beitrag zur gesamtstaatlichen Sicherheitsvorsorge
- Zusammenführung CERTs in Bw

Operationen + Beitrag Multinationales Command Element



Aufbau Fähigkeiten im Kommando CIR:

- Planung und Führung von Operationen im CIR
- Beiträge zu einem multinationalen Command-Element

Zentrum Cyber Operationen



- Stärkung der vorhandenen Fähigkeiten zu Cyber Operationen (CNO)
- Cyber-Lage (gegnerische Fähigkeiten)
- Red-Teaming als Beitrag zum Schutz

Gemeinsames Lagezentrum CIR



Aufbau Fähigkeiten im Kommando CIR:

- Bundeswehrgemeinsames Lagebild (ohne Anteile der eigenen Lage anderer Organisationsbereiche)
- Ressortübergreifende Zusammenarbeit

Zentrum Software Kompetenz IT-System Bw



- Ausbau Kompetenz zu Beratung, Entwicklung und Integration im Bereich Software
- Beitrag zur Bereitstellung innovativer Lösungen

Zentrum Nachrichtenlage



- in Breite und Tiefe weiterentwickelte militärische Nachrichtenlage
- Operations Research und Simulation

Ausbau Stab Kommando CIR



- Konzentration der Aufgabenwahrnehmung in der Dimension CIR
- Stärkung der Fachaufgaben Planung und Recht

Zentrum für Geoinformations wesen der Bundeswehr



- Ausbau Unterstützung Lagebild und Operationsplanung mit Fähigkeiten zu Big Data Analyse
- Verbesserung Navigationsfähigkeiten (alternative Navigation)

Entscheidung Verteidigungsministerin

Pressemitteilung vom 14.10.2016



 Bundesministerium
der Verteidigung

**Presse-
mitteilung**

HAUPTABTEILUNG BMVg
STAB
POSTADRESSE 11055
TEL. +49 (0) 30 1809-1
FAX +49 (0) 30 1809-1000
INTERNET www.bmvg.bund.de
E-MAIL bmvg@bundeswehr.de

DATE: Berlin, 14. Oktober 2016
SEITE: 1 von 2
NUMMER: 11/2016

**Von der Leyen nominiert Leinhos
als ersten Cyber-Inspekteur der Bundeswehr**
Generalmajor Leinhos soll ab April 2017 neuen militärischen
Organisationsbereich leiten

Bundesverteidigungsministerin Ursula von der Leyen hat den derzeitigen Leiter des Aufbaustabes Cyber- und Informationsraum (CIR), Generalmajor Ludwig Leinhos, für die Führung des neu aufzustellenden Kommandos CIR bestimmt. Er wird diese Funktion ab dem 1. April 2017 wahrnehmen. Das neue Kommando CIR in Bonn soll rund 300 Dienstposten haben. Zum gesamten neuen militärischen Organisationsbereich CIR sollen 13.500 Dienstposten gehören, die größtenteils aus anderen Teilstreitkräften und Organisationsbereichen der Bundeswehr in die neue Struktur überführt werden.

Nach der Aufstellung der neuen Ministeriumsabteilung Cyber- und Informationstechnik (CIT) am 5. Oktober 2016 in Berlin ist dies ein weiterer wesentlicher Schritt der Bündelung der Fähigkeiten der Bundeswehr im Cyber- und Informationsraum und der operativen Steuerung der Digitalisierungsprojekte der Truppe. Im April 2017 wird dann der neue militärische Organisationsbereich CIR mit Sitz in Bonn seine Arbeit aufnehmen. Der neu ernannte Inspekteur Leinhos ist dann den Spitzenmilitärs des Heeres, der Luftwaffe, der Marine, der Streitkräftebasis und des Sanitätsdienstes der Bundeswehr gleichgestellt.

Generalmajor Ludwig Leinhos weist exzellentes Fachwissen für die Führung dieses neuen Bereiches auf. Er ist 60 Jahre alt und trat 1975 in die Bundeswehr ein. Ursprünglich aus dem Bereich der Elektronischen Kampfführung stammend, war sein militärischer Werdegang von verschiedenen Führungsverantwortungen im In- und Ausland im Bereich Führungssysteme, IT-Planung und Anwendung geprägt. Bevor er am 1. Juli 2016 Leiter des Aufbaustabes CIR wurde, war Leinhos Verantwortlicher für Cyber Defence im NATO Hauptquartier in Brüssel. Er ist verheiratet und hat zwei Söhne.

Inspekteur CIR

- BM´in Ursula von der Leyen hat den derzeitigen Leiter des Aufbaustabes Cyber- und Informationsraum (CIR), **Generalmajor Ludwig Leinhos**, für die Führung des neu aufzustellenden Kommandos CIR bestimmt.





Stufenweise Umsetzung des militärischen OrgBereichs CIR

Schritt 1 IOC

Aufstellung milOrgBer

- Neuer OrgBer mit Anfangsbefähigung (truppendienstliche Führung)
- Abstützung auf SKB

2017



Crawl

Zwischenschritt 2 IOC+

Ausbau milOrgBer

- Neuer OrgBer mit truppendienstlicher Zielbefähigung und Bündelung der planerischen Expertise

2018+



Walk

Schritt 3 FOC

Einnahme Zielstruktur

- KdoCIR erreicht FOC
- Mehrwerte in Abhängigkeit von Personal

2021+

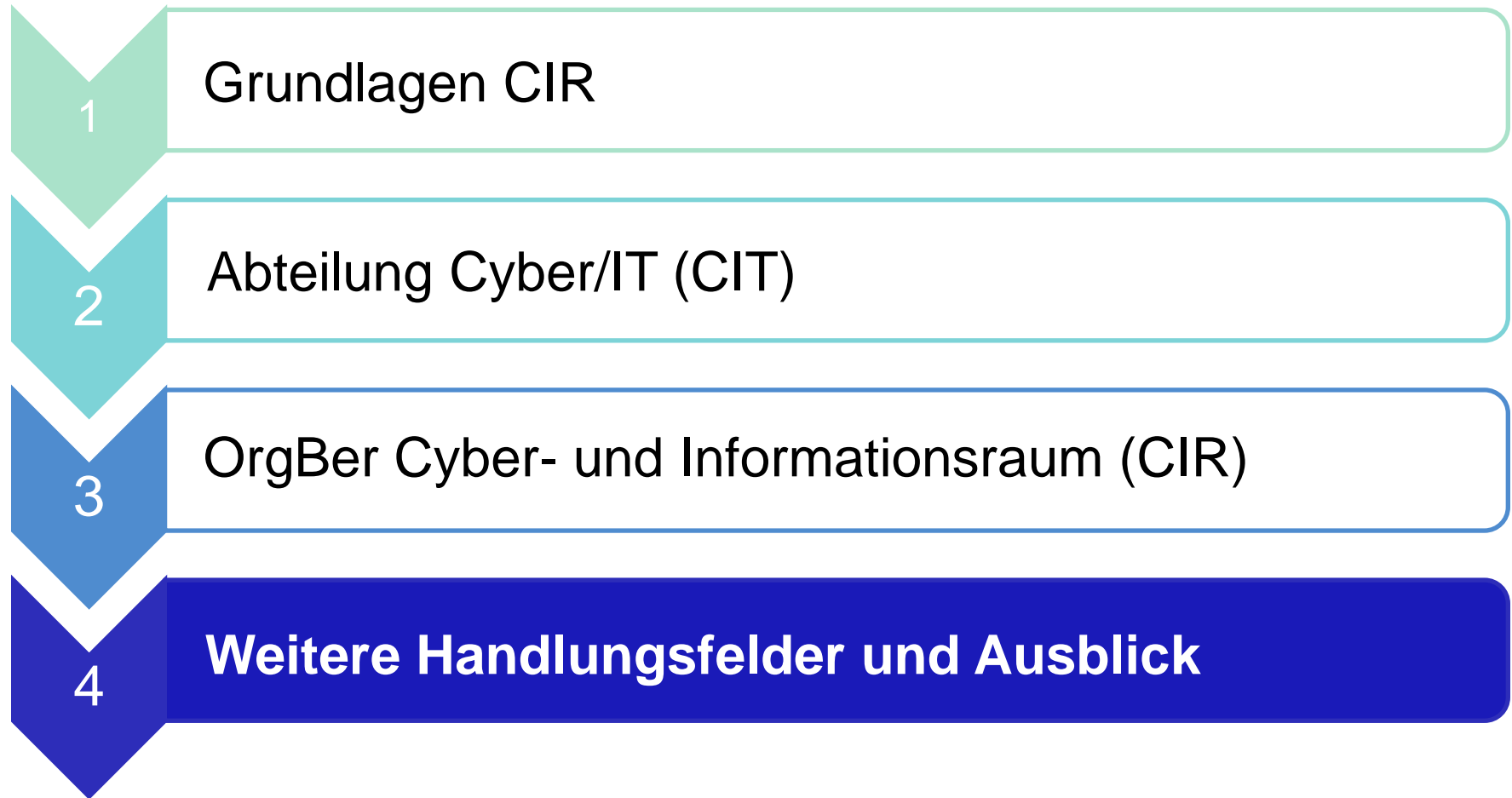


Run

Status: Alle Arbeiten im Zeitplan!



Gliederung





Mit Quick Hits sollen schnell Mehrwerte erreicht werden (I)

Quick Hits...

...und ihre Mehrwerte

**Cyber-Cluster
Universität der Bundeswehr München**

Anstoß von Produktvorhaben aus hochwertiger universitärer Forschung bei gleichzeitiger Koppelung an wissenschaftliche Ausbildung

**Einrichtung internationaler und ressort-
übergreifender Master-Studiengang
Cyber-Sicherheit**

Stärkung Attraktivität Bundeswehr für die Zielgruppe und gesamtstaatlicher Beitrag zur Deckung des Mangels an hochqualifiziertem Personal

Cyber Hygiene Check Up

Verbesserung der Sensibilisierung für Risiken der Digitalisierung sowie Verbesserung der Informationssicherheit

Werkstattgespräche Cyber-Sicherheit

Gewährleistung der übergreifenden Zusammenarbeit bei der gesamtstaatlichen Sicherheitsvorsorge



Mit Quick Hits sollen schnell Mehrwerte erreicht werden (II)

Handlungsfeld **Beschaffung & Innovation**

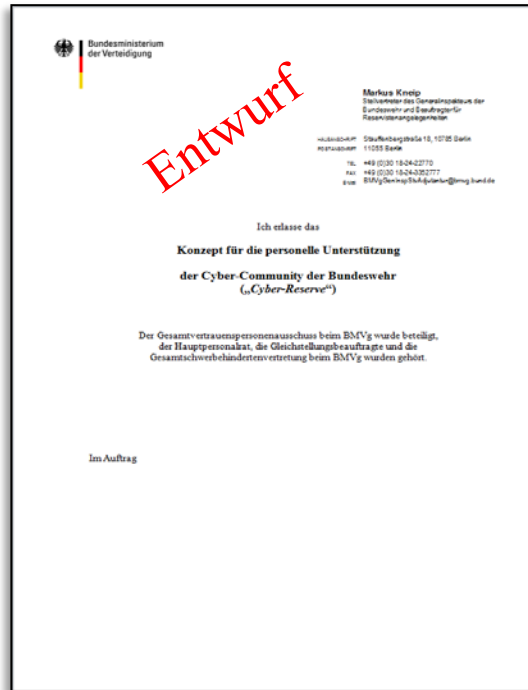
schnellere Verfügbarkeit von
Produkten und Innovationen durch
gezielte Förderung von Forschung und Technologie

**Trendwende Personal +
Werbekampagne**

Zukünftige Verfügbarkeit von Dienstposten
eingeleitet und Bekanntheitsgrad mit
interessanter Werbekampagne erhöht

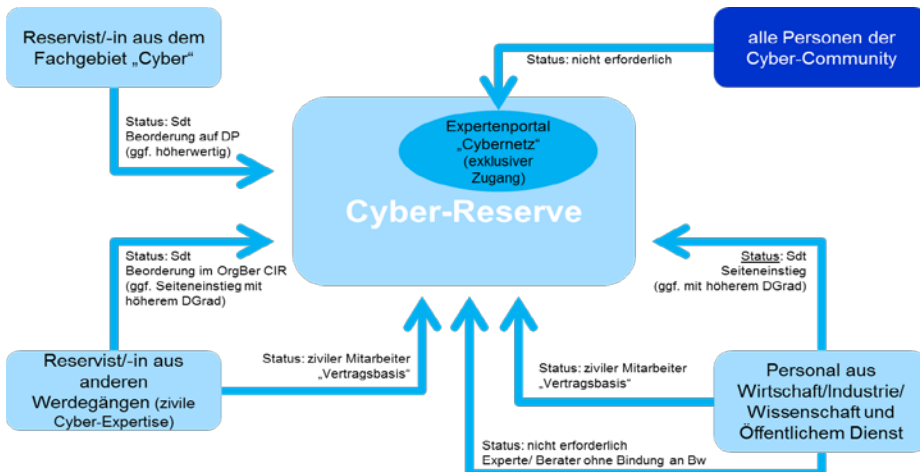
Cyber-Reserve

Abrufbarkeit ungenutzter Potenziale sowie
Anreicherung eigener Fähigkeiten durch Cyber-
Spezialisten aus Wirtschaft & Gesellschaft



Primäre Ziele:

- Bereitstellung von Cyber-Fachkräften für Schwerpunkte im Bereich CIR
- Bündelung von Spezialisten und Spezialistinnen, um durch gemeinsames Üben eine wirkungsvolle und state-of-the-art Cyber-Wirkkomponente, ggf. auch mit internationalen Verbündeten aufzubauen.
- Bildung eines zusätzlichen Kräfteelements im Inland, um für die Abwehr von schwerwiegenden Cyber-Angriffen zur Verfügung zu stellen.
- Förderung des Erfahrungsaustausches von eigenen Cyber-Spezialisten und Cyber-Spezialistinnen mit entsprechenden Spezialisten und Spezialistinnen außerhalb der Bundeswehr durch Community-Bildung





Cyber-Cluster Universität der Bundeswehr München

Testen & Labore

Forschung

Vernetzung

Entwicklung von
Sicherheitslösungen

Beratung



wissenschaftliche
Ausbildung

Fort- und
Weiterbildung



Personal

- Entwicklung von Karrierewegen und Laufbahnen
- Konzeptionelle Weiterentwicklung der Fort-, Aus- und Weiterbildung
- Einführung Cyberstipendien
- Weiterentwicklung monetärer Anreize



- Verstärkte Gewinnung von Seiteneinsteigern
- Weiterentwicklung der existierenden Kompetenzbereiche FüUstg und MilNw
- Prüfen von neuen Methoden zur Personalgewinnung/-auswahl Instrumente (Assessment, IT-Camp, ...)



Der Cyber- und Informationsraum hat sich zur 5. militärischen Dimension entwickelt – und fordert die Bw



Vom „Hype“...



“If we're going to be connected, then we need to be protected. Cyber [...] is our country's biggest threat.”
(Barack Obama, 2015)

“ Cyber-attack can trigger Article 5 collective defence; because we regard cyber as potentially as dangerous as a conventional attack.”
(Jens Stoltenberg, 2015)

...zur Realität.

DEUTSCHLANDS
FREIHEIT
WIRD AUCH IM
CYBERRAUM
VERTEIDIGT.
MACH, WAS WIRKLICH ZÄHLT.

PROJEKT
DIGITALE
KRÄFTE
Bundeswehr
bundeswehrkarriere.de



Perspektiven und Herausforderungen im zukünftigen OrgBer Cyber- und Informationsraum (CIR)

Oberst i.G. Fleischmann

ChdSt Aufbaustab Cyber- und Informationsraum



Von der Herausforderung zu neuen Fähigkeiten

Gestern

Morgen

Zersplitterte und verteilte Zuständigkeit für IT im BMVg
– Cyber nicht umfassend abgebildet –

Gebündelte und eindeutige Zuständigkeit in der
Abteilung Cyber/ IT im BMVG

Dimension Cyber- und Informationsraum
in der Bundeswehr **nicht bedeutungsgerecht**
wahrgenommen

Dimension Cyber- und Informationsraum **im eigenen**
Organisationsbereich zusammengefasst

Betrieb und **Schutz** des IT-Systems der Bundeswehr in
den Bereichen Rüstung und Streitkräfte **verteilt**

Betrieb und **Schutz** des IT-Systems
der Bundeswehr **in einer Hand**

Cyber- und Informationsraum in einer **unterstützenden**
Funktion im Rahmen **klassischer Operation**

Wirken im Cyber- und Informationsraum auch
als **eigenständige Operation**

Herausforderungen im Bereich der
Nachwuchsgewinnung

Neue, attraktive Arbeitsplätze und **fokussierter**
Auftritt im Recruiting

Einführung von IT nach dem **Standardverfahren** für
Großprojekte

Agile Planungs- und Einführungsverfahren zur
Steigerung der Innovationsfähigkeit im **Bereich IT**