Bundeswehr
Wir. Dienen. Deutschland.

Aufgabenstellung und Herausforderungen der Bundeswehr im Cyber- und Informationsraum

Politisches Bildungsforum Thüringen

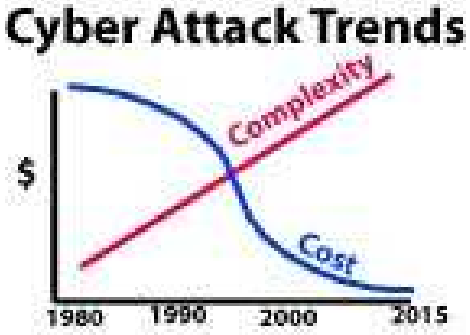
18. Oktober 2017

Generalmajor Michael Vetter
Stellvertretender Inspekteur CIR und Chef des Stabes KdoCIR

Zukünftige strategische sicherheitspolitische Faktoren

Cyber Bedrohungen

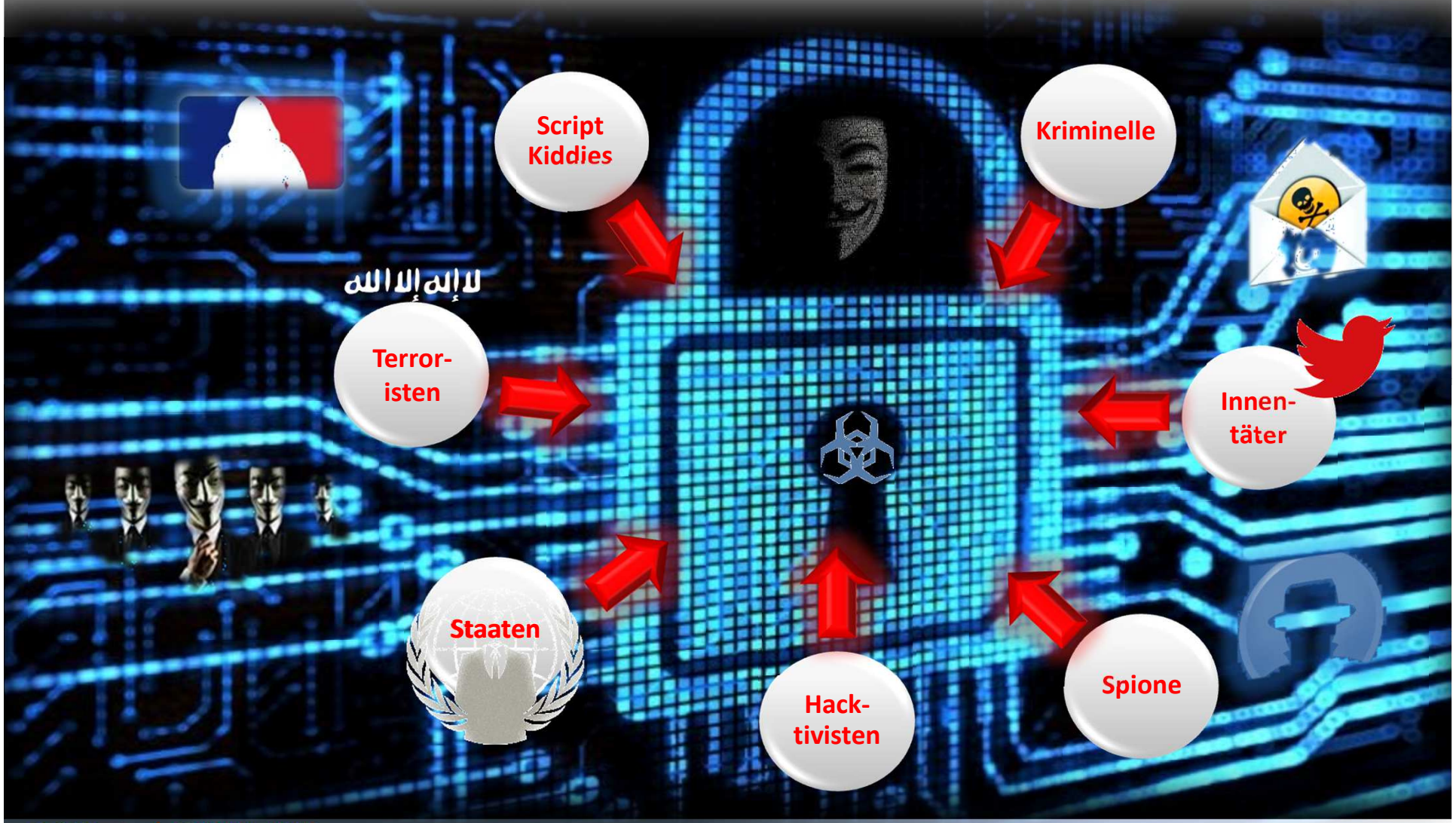
- Angriffs-Komplexität: ↗
  Angriffs-Aufwand: ↘



- Niedrige Eintrittsschwelle und schwierige **Attribution**

- Steigende Verwundbarkeit der Gesellschaften durch Digitalisierung und Vernetzung

Akteure

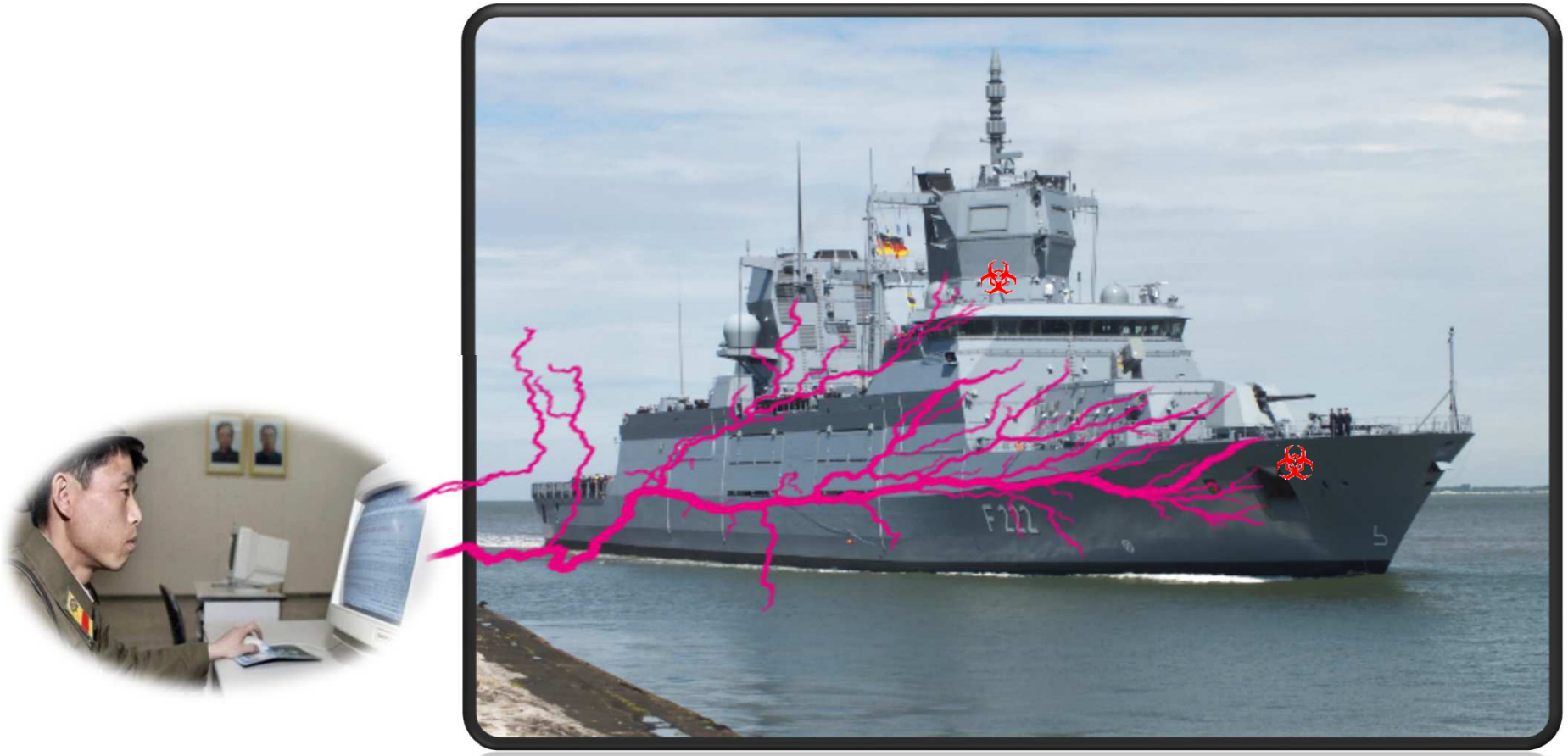

Script Kiddies
Kriminelle
لاإله إلاالله
Terror-isten
Innen-täter
Staaten
Hack-tivisten
Spione

Cyber durchdringt alle Bereiche der Bundeswehr

- Bürokommunikation
- Führungsinformationssystem
- Waffensysteme
- Gesundheitsversorgung
- Personalmanagement
- Rechnungswesen
- Logistik, Lieferketten
- ....usw.

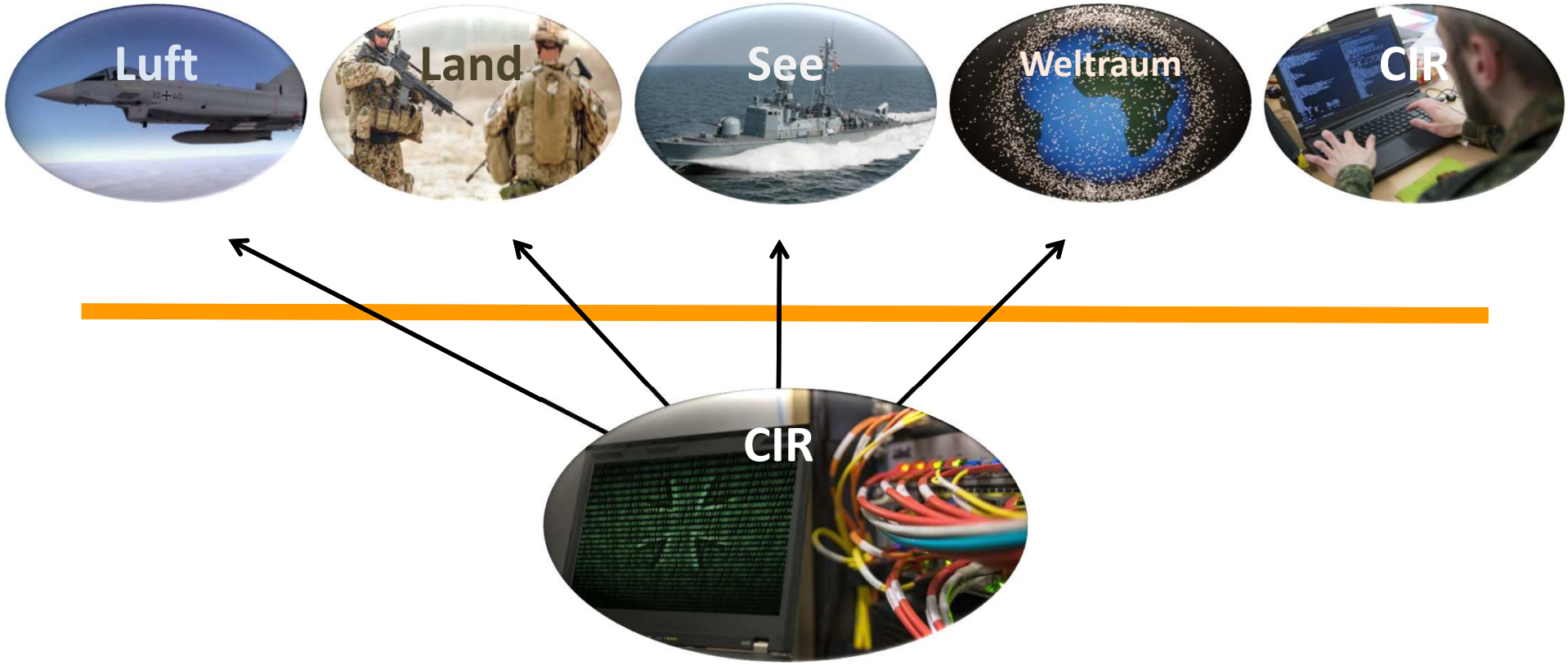
Cyber Bedrohungen

David vs. Goliath Problem



Die fünfte Dimension
Cyber- und Informationsraum

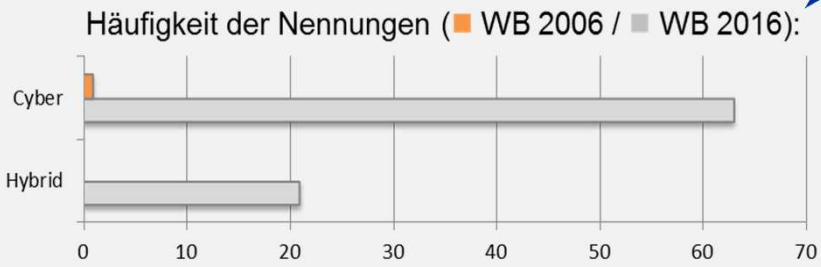
Wirkebene



„Enabler“

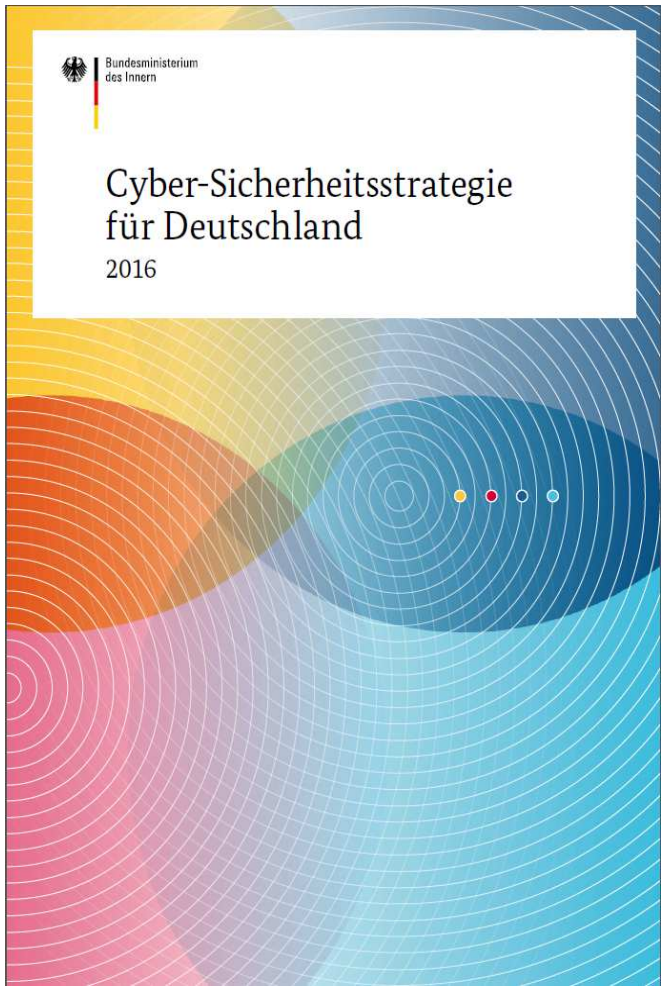
Weißbuch 2016

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.

Cyber-Sicherheitsstrategie für Deutschland 2016



<u>Auswirkungen für die Bundeswehr</u>

- Deutlich stärkere Rolle der Bundeswehr in der gesamtstaatlichen Sicherheitsvorsorge
- Schutz Kritischer Infrastrukturen als ressortgemeinsame Aufgabe
- Auf- und Ausbau eines Cyber-Clusters bei UniBw M
- **Weiterentwicklung des Cyber-AZ mit stärkerer Bw- Beteiligung**
- 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)

Beitrag der Bundeswehr

Militärischer Abschirmdienst (MAD)

Central Monitoring CERT- BWI

IT-Sicherheit Organisation

Computer Netzwerk Operations (CNO)

Aufgaben

- Verfassungsrechtlicher Auftrag zur Verteidigung DEU
- Abwehr von Bedrohungen im Cyber-Raum ggü Streitkräften
- Betrieb und Schutz eigener IT-Anteile zur Gewährleistung militärischer Handlungs- und Führungsfähigkeit sicherstellen
- Nutzung Cyber-Raum durch gegnerische Kräfte einschränken, ggf. unterbinden
- Einsatz der Bundeswehr zur Bewältigung eines besonders schweren Unglücksfalls (Amtshilfe nach Art. 35 GG)

Quelle: Strategische Leitlinie „Cyber-Verteidigung“ vom 16.04.15

Wesentliche Säulen des OrgBer CIR

- Schutz und Betrieb des IT-Systems der Bundeswehr (neue Dauereinsatzaufgabe)
- MilNW als Dauereinsatzaufgabe
- Aufklärung und Wirkung im CIR (elektromagnetisches Spektrum, Cyberraum und Informationsumfeld)
- GeoInfo-Unterstützung als Enabler (u.a. Raumbezug als Basis und Scharnier zwischen CIR und anderen Dimensionen)
- Beitrag zur gesamtstaatlichen Cybersicherheit/-verteidigung

CIR-relevante Fähigkeiten werden zusammengeführt

Militärisches Nachrichtenwesen

FmElo-Aufklärung

Elektronische Gegenmaßnahmen

Computer Netzwerk Operationen

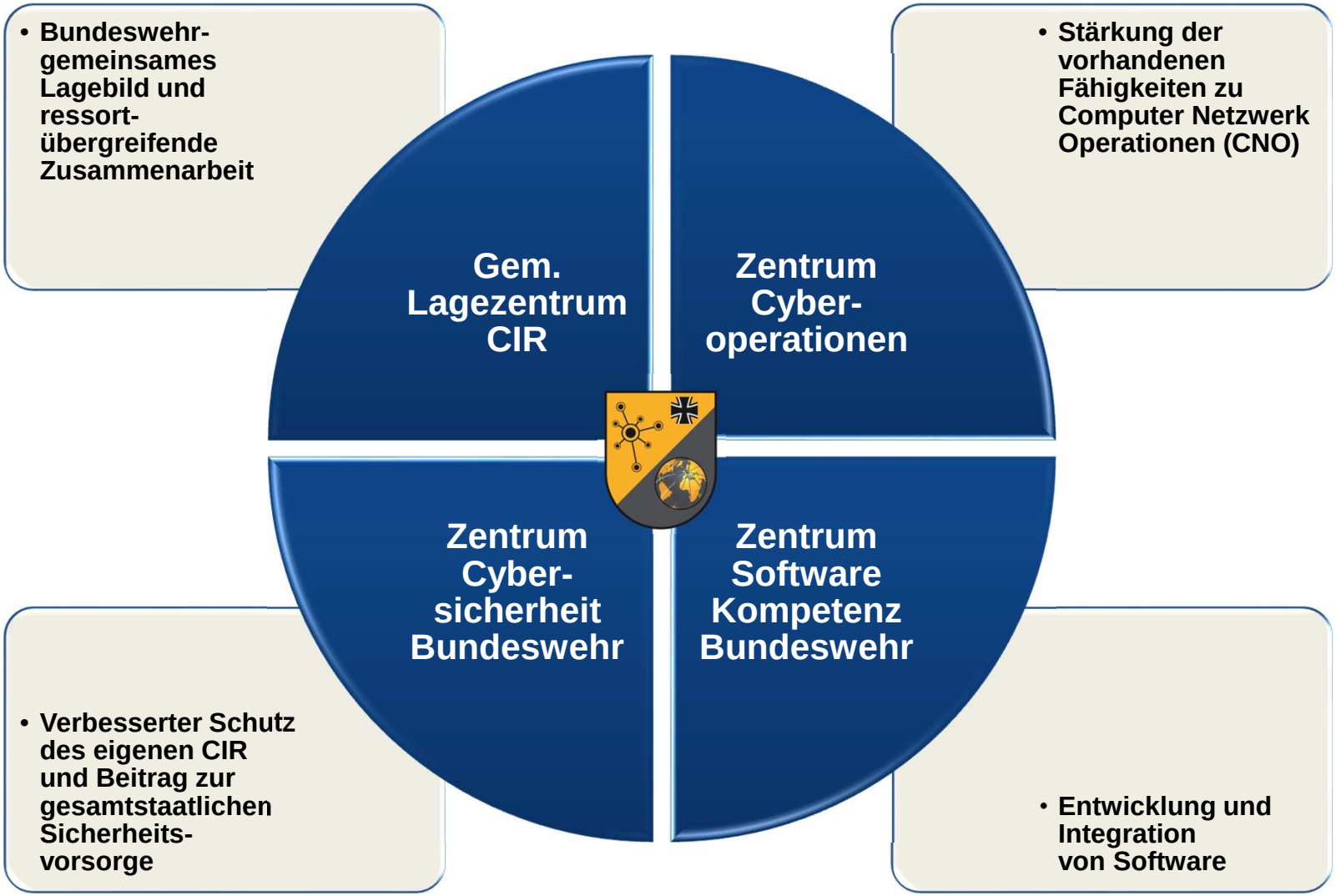
GeoInformationswesen

IT-Unterstützung

Cyber-/Informationssicherheit

Operative Kommunikation

Neue Cyberfähigkeiten im CIR

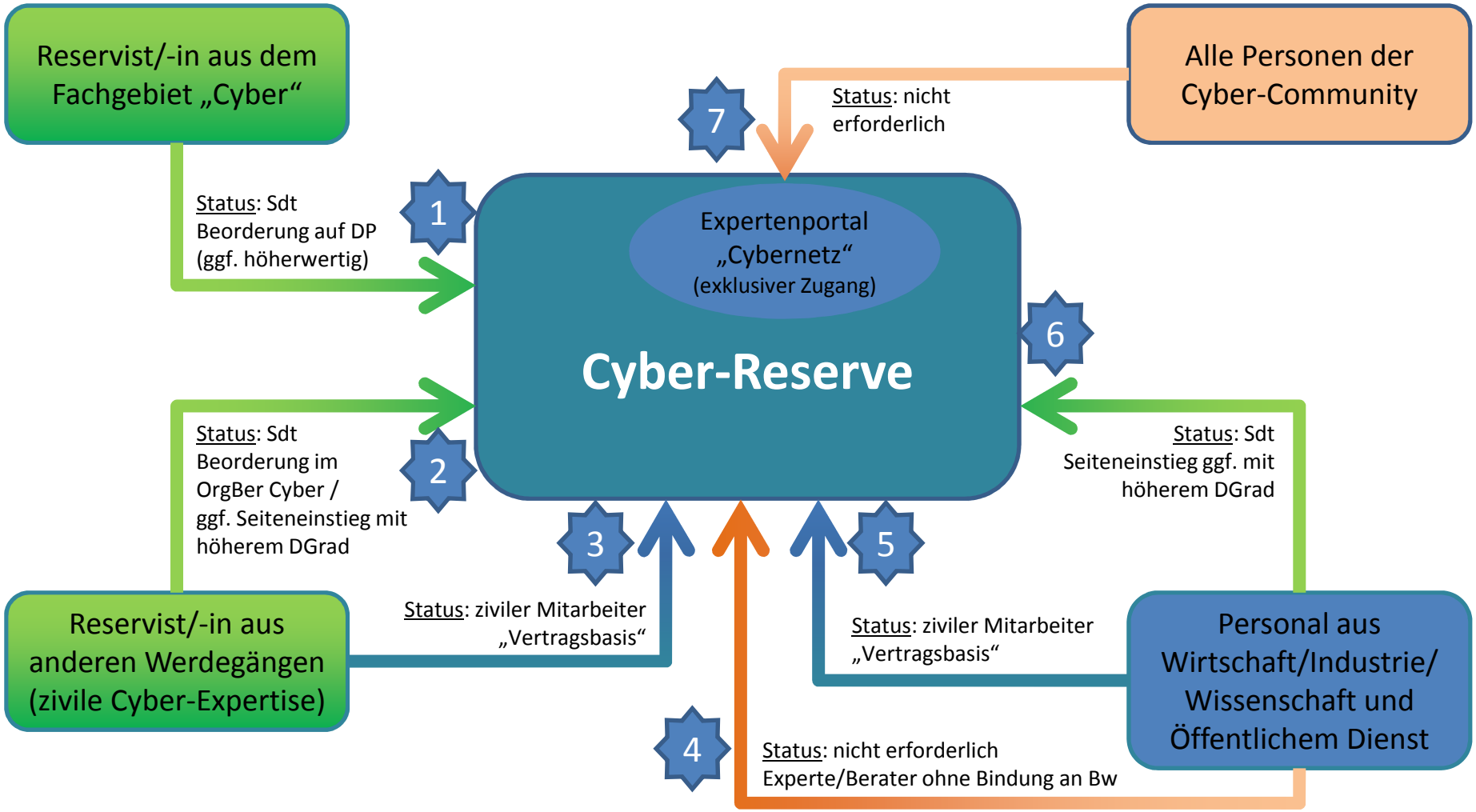


Personal

- 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, …)

„Cyber-Reserve“ Personal-Pool



Cyber-Cluster

Universität der Bundeswehr München

Testen & Labore

Forschung

Vernetzung

Entwicklung von Sicherheitslösungen

Beratung

wissenschaftliche Ausbildung

Fort- und Weiterbildung

Fazit

- Die Tragweite der gesellschaftsrelevanten und sicherheitspolitischen Entwicklungen der neuen Dimension *Cyber – und Informationsraum* wird häufig noch immer unterschätzt.
- Cybersicherheit und Resilienz ist eine gesamtstaatliche Aufgabe der wir uns alle annehmen müssen.
- Der neue Organisationsbereich ***CIR*** der Bundeswehr stellt sich den militärischen Herausforderungen im Cyber- und Informationsraum und trägt zur gesamtstaatlichen Cybersicherheit bei.